**SUPERIOR COURT OF THE STATE OF CALIFORNIA**
**FOR THE COUNTY OF LOS ANGELES**

***Social Media Cases***
**JCCP5255**
**(Lead Case: 22STCV21355)**

**Dept. 12 SSC**
**Hon. Carolyn B. Kuhl**

**Defendants' Motion to Strike Third-Party Misconduct and Online Challenge Allegations from Identified Short-Form Complaints**

Court's Ruling: The court grants the Motion to Strike in part, denies it in part, and denies it without prejudice in part as discussed in the opinion below.

## I. FACTUAL AND PROCEDURAL BACKGROUND

Plaintiffs in these coordinated proceedings are minor users of social media platforms (or parents of those users) who allege they have suffered various types of harm resulting from use of the platforms. Plaintiffs bring their claims against multiple Defendants that designed and operated the following social media platforms: Facebook, Instagram, Snapchat, TikTok, and YouTube.[1] The Master Complaint in this case, filed May 16, 2023, consists of 300 pages. Each Plaintiff or family in this coordinated proceeding also filed a short-form complaint that adopts some or all of the allegations of the Master Complaint, specifies each Plaintiff's injuries, and adds individual allegations concerning the social media platforms used by each Plaintiff and how those platforms injured him or her.

[1] Facebook and Instagram are owned, designed, and operated by a group of Defendants who are referred to collectively herein as "Meta." Snapchat is owned, designed, and operated by Defendant Snap Inc. (Snap). TikTok is owned, designed, and operated by multiple Defendants who are referred to collectively herein as "ByteDance." YouTube is owned, designed, and operated by multiple Defendants referred to collectively herein as "Google."

Defendants previously demurred to the Master Complaint and to three typical short-form complaints. In a ruling issued on October 13, 2023 (October 2023 Ruling), this court sustained the demurrer as to a number of causes of action, including Plaintiffs' product liability causes of action, but overruled the demurrer as to the negligence cause of action pleaded against all Defendants and the fraudulent concealment claim pleaded against Meta. The October 2023 Ruling includes an extended summary of the allegations of the Master Complaint. (October 2023 Ruling, at pp. 2-11.)

One of Defendants' principal arguments in the briefing on the demurrer to the Master Complaint was that Section 230 of the Communications Decency Act, 47 U.S.C. § 230 (Section 230) bars liability for the claims alleged by Plaintiffs. As discussed further below, Section 230 provides immunity for a provider of an interactive computer service (such as Defendants) against liability for speaking or publishing third-party content. The court overruled the demurrer to the negligence claim because the Master Complaint set forth "several theories of breach of duty ... that are not barred by Section 230" (October 2023 Ruling, at p. 57), although the court recognized that some allegations of the Master Complaint "can be read to seek to hold Defendants liable for publishing third-party content" (*id.* at p. 66).

Defendants now move to strike numerous allegations of the Master Complaint that Defendants contend are barred by Section 230 immunity or by the First Amendment. In part, the Motion to Strike addresses a gap in the briefing of the Demurrer to the Master Complaint. None of the short-form complaints included in the coordinated briefing on that Demurrer included injuries allegedly caused by child predators, by child sexual abuse material or by dangerous "challenges" found on social media. (See October 2023 Ruling, at p. 11, fn. 1.)

The factual allegations that Defendants seek to strike from the Master Complaint may be grouped into the following categories:

(1) Failure to warn.
(2) Failure to remove Child Sexual Abuse Material (CSAM) and failure to create processes to report CSAM.
(3) Recommendation of inappropriate content to minors.
(4) Creating a geolocation feature that allows strangers access to data by which minors can be located.
(5) Affirmatively recommending that minors contact strangers.
(6) Creating systems to allow strangers to send cash to minors and reward minors with "virtual gifts."

(7) Encrypting direct messages between minors and strangers.
(8) Creating a means by which users can make images they create or see disappear.
(9) Inadequate mechanisms for age verification.
(10) Setting minors' accounts to "public" as a default.

The court and the parties also agreed that seven short-form complaints would be addressed by the current motion, and Defendants have moved to strike portions of each of these individual complaints. The seven short-form complaints that are relevant to this proceeding are:

(1) First Amended Short Form Complaint For Damages And Demand For Jury Trial, *A.S. ex rel. E.S. v. Meta Platforms, Inc., et al.*, Case No. 22STCV28202 (L.A. Super. Ct. filed Jan. 5, 2024) (referred to herein as "A.S. SFC").
(2) First Amended Short Form Complaint For Damages And Demand For Jury Trial, *GlennMills v. Meta Platforms, Inc., et al.*, Case No. 23SMCV03371 (L.A. Super. Ct. filed Jan. 5, 2024) (referred to herein as "Glenn-Mills SFC").
(3) First Amended Short Form Complaint For Damages And Demand For Jury Trial, *K.L. ex rel. S.S. v. Meta Platforms, Inc., et al.*, Case No. CIV SB 2218921 (L.A. Super. Ct. filed Jan. 5, 2024) (referred to herein as "K.L. SFC").
(4) First Amended Short Form Complaint For Damages And Demand For Jury Trial, *N.S. ex rel. Z.H. v. Snap Inc.*, Case No. 22CV019089 (L.A. Super. Ct. filed Jan. 5, 2024) (referred to herein as "N.S. SFC").
(5) First Amended Short Form Complaint For Damages And Demand For Jury Trial, *P.F. ex rel. A.F. v. Meta Platforms, Inc., et al.*, Case No. 23SMCV03371 (L.A. Super. Ct. filed Jan. 5, 2024) (referred to herein as "P.F. SFC").
(6) Second Amended Short Form Complaint For Damages And Demand For Jury Trial, *J.S. and D.S. ex rel. L.H.S. v. Meta Platforms, Inc., et al.*, Case No. CV2022-1472 (L.A. Super. Ct. filed Jan. 9, 2024) (referred to herein as "J.S. SFC").
(7) Second Amended Short Form Complaint For Damages And Demand For Jury Trial, *K.K. ex rel. S.K. v. Meta Platforms, Inc., et al.*, Case No. 23SMCV03371 (L.A. Super. Ct. filed Jan. 17, 2024) (referred to herein as "K.K. SFC").

Six of these short-form complaints allege that, in addition to harms such as "addiction/compulsive use," "depression," and "anxiety," Plaintiffs also suffered "[e]xploitation and/or sexual abuse related harms." (See, e.g.,

A.S. SFC, at pp. 4-5.) The J.S. SFC alleges the following additional harms: "[h]arms resulting from being the victim of viral challenges engaged in by other minors." (J.S. SFC, at p. 5.) Defendants move to strike the allegations of harm from exploitation or sexual abuse and from viral challenge videos.

## II. DISCUSSION

### A. Plaintiffs' Procedural Objections

#### *1. The Motion to Strike is Timely*

A motion to strike a complaint must be filed within the time allowed for filing an answer; and a motion to strike a complaint should be heard at the same time as a demurrer to that complaint. (See Code Civ. Proc., § 435, subd. (b)(1); Cal. Rules of Court, rule 3.1322, subd. (b).) Plaintiffs argue that this Motion to Strike should have been filed and heard in connection with Defendant's demurrer to the Master Complaint.

Plaintiffs' position is not well taken. Here, Defendants have moved to strike the allegations of seven short-form complaints, filed in January, which incorporate the factual allegations of the Master Complaint. Defendants' motion to strike allegations in the seven short-form complaints is timely. Plaintiffs' incorporation of the factual allegations of the Master Complaint into the short-form complaints also makes the allegations in the Master Complaint properly subject to Defendants' Motion to Strike.

##### *a. The Motion to Strike is Procedurally Proper*

Plaintiffs argue it is procedurally improper for this court to strike portions of the operative pleadings that Defendants claim seek to hold them liable qua publishers in contravention of the immunity provided by Section 230. This argument is not supported by California procedure and practice.

This court may "[s]trike out any irrelevant, false, or improper matter inserted in any pleading." (Code Civ. Proc., § 436, subd. (a).) The First District Court of Appeal has instructed that trial courts may, in the interests of judicial efficiency and fairness to the defendant, strike portions of a cause of action that are "substantively defective." (*PH II, Inc. v. Superior Court* (1995) 33 Cal.App.4th 1680, 1682.) Furthermore, in these coordinated proceedings involving the claims of hundreds of Plaintiffs, this court "has broad discretion ... to fashion suitable methods of practice in order to manage complex litigation." (*Fire Ins. Exchange v. Superior Court* (2004) 116 Cal.App.4th 446, 452.) An order striking any allegations that are clearly

barred by Section 230 is a proper and appropriate manner of managing this litigation and providing needed clarity regarding the substantive viability of Plaintiffs' claims. Striking the improper matter in the operative pleadings is also consistent with Section 230's policy goal of preventing the threat of litigation from chilling speech posted by service providers on the internet. (See, e.g., *Barrett v. Rosenthal* (2006) 40 Cal.4th 33, 44 (*Barrett*).)

Nevertheless, "[w]here the defect raised by a motion to strike or by demurrer is reasonably capable of cure, leave to amend is routinely and liberally granted to give the plaintiff a chance to cure the defect in question." (*CLD Construction, Inc. v. City of San Ramon* (2004) 120 Cal.App.4th 1141, 1146, internal citations and quotation marks omitted.) In this litigation, this court sustained a demurrer with respect to a negligent failure to warn claim Plaintiffs attempted to plead in seven short-form complaints that were selected as sample pleadings. (Ruling, Mar. 27, 2024.) The court granted leave to amend to allow Plaintiffs to plead additional facts in support of their asserted cause of action for negligent failure to warn, and the deadline for the amendment had not yet passed when this Motion to Strike was briefed. Insofar as the current Motion to Strike seeks to eliminate factual allegations concerning failure to warn, the court declines to strike those allegations and will consider Defendants' objection to them in the context of any pleading challenge that may be brought to any amended claim for negligent failure to warn. To do otherwise would be to effectively deny Plaintiffs a right to amend. Therefore, the Motion to Strike paragraphs 137-138, 369-370, 518, 626, 662, 774, 781-782, and 809 is denied without prejudice.

B. Section 230 and General Principles Governing Its Application

Defendants' principal argument in support of the Motion to Strike is that Section 230 provides immunity to Defendants that bars Plaintiffs from holding Defendants liable based on the allegations challenged by this Motion. As this court did in its October 2023 Ruling, the court again sets forth the specific statutory language on which Defendants base their immunity claim, and the guiding legal authorities that frame the scope of Section 230 immunity.

Section 230, titled "Protection for private blocking and screening of offensive material," was passed by Congress in 1996. In part, the statute was meant to overrule a decision of a New York state court that had held an internet service provider liable as a publisher of offensive content because it deleted some offensive message board posts and not others. (See *Doe v. Internet Brands, Inc.* (9th Cir. 2016) 824 F.3d 846, 851-852 (*Internet Brands*); *Hassell v. Bird* (2018) 5 Cal.5th 522, 534 (*Hassell*).) Congress sought to spare internet service providers the "grim choice" between doing

nothing to remove offensive content and removing some but not all offensive content. (*Internet Brands*, at p. 852.)

In a subdivision of Section 230 titled "Protection for 'Good Samaritan' blocking and screening of offensive material,"[2] Section 230 states that no provider of an interactive computer service may be held liable for either (a) a voluntary good faith action to restrict access to materials that the provider considers "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable," or (b) any action to enable information content providers or others the technical means to restrict access to such materials. (47 U.S.C. § 230, subd. (c)(2)(A)-(B).) Under that same heading, Congress provided additional protection for information service providers, which has proven more difficult to interpret:

> Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(*Id.* § 230, subd. (c)(1).)

Defendants seek protection from the claims asserted in this case based on this language of Section 230. It is conceded by all parties that Defendants are "provider[s] ... of an interactive computer service" within the meaning of subdivision (c)(1) of Section 230.[3]

Congress expressly stated its policy goals in enacting Section 230. Subdivision (b) of Section 230 states "[i]t is the policy of the United States" to promote continued development of the internet and interactive computer services and "to preserve the vibrant and competitive free market" of these services "unfettered by Federal or State regulation." (*Id.* § 230, subd. (b)(1)-(2).) Congress equally desired "to encourage the development of technologies which maximize user control over what information is received

---

[2] The court in *Internet Brands*, *supra*, 824 F.3d at p. 851, looked to the heading of subdivision (c) of Section 230 to guide its consideration of the purposes of Section 230.

[3] "The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." (*Id.* § 230, subd. (f)(2).)

"The term 'access software provider' means a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." (*Id.* § 230, subd. (f)(4).)

by individuals, families and schools" using interactive computer services and to "remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict children's access to objectionable or inappropriate online material." (*Id.* § 230, subd. (b)(3)-(4).) Congress also expressed a policy "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." (*Id.* § 230, subd. (b)(5).)

The California Supreme Court has quoted with approval Ninth Circuit precedent recognizing that "there is an apparent tension between Congress's goals of promoting free speech while at the same time giving parents the tools to limit the material their children can access over the Internet ... . The need to balance competing values is a primary impetus for enacting legislation. Tension within statutes is often not a defect but an indication that the legislature was doing its job." (*Barrett*, *supra*, 40 Cal.4th at p. 56, internal citations, quotation marks, and brackets omitted, quoting *Batzel v. Smith* (9th Cir. 2002) 333 F.3d 1018, 1028 (*Batzel*), reversed on other grounds by subsequent statutory amendment as stated in *Breazeale v. Victim Services, Inc.* (9th Cir. 2017) 878 F.3d 759, 766-767).

As to the preemptive effect of Section 230, the statute states:

> (e) Effect on other laws.
>
> ...
>
> (3) State law. Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

(47 U.S.C. § 230, subd. (e)(3).)

Several general principles can be derived from caselaw that has evolved since the enactment of subdivision (c)(1) of Section 230:

- A provider of interactive computer services (hereinafter sometimes referred to as "a provider") cannot be held liable as a publisher or speaker of content provided by a third party. (*Barrett*, *supra*, 40 Cal.4th at p. 57 ["Congress intended to create a blanket immunity from tort liability for online republication of third party content"]; *Zeran v. America Online, Inc.* (4th Cir. 1997) 129 F.3d 327, 330 ["By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information

originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role"].)

- A provider also cannot be liable for incidental editorial functions because it is still acting as a publisher of third-party content. (*Batzel, supra*, 333 F.3d at 1031 [provider who does no more than select and make minor edits to third-party content cannot be considered a content provider].)

- A provider can be liable for its own speech, subject to First Amendment restrictions. (*Fair Housing Council v. Roommates.com, LLC* (9th Cir. 2008) 521 F.3d 1157, 1169 (en banc) (*Roommates*) [Section 230 did not bar liability where a provider "designed its search and email systems to limit the listings available to subscribers based on sex, sexual orientation and presence of children" and thereby allegedly engaged in unlawful discriminatory conduct]; *Liapes v. Facebook, Inc.* (2023) 95 Cal.App.5th 910 (*Liapes*) [Facebook acted as a "content developer" and therefore Section 230 did not bar a claim against Facebook for unlawful discrimination under California law. Facebook allegedly required users to disclose age and gender and then relied on those "unlawful criteria" to develop an advertising targeting and delivery system making it difficult for individuals with protected characteristics (women and older people) to find or access insurance ads on Facebook].)

- It is important to consider the gravamen of the cause of action brought against the provider. Section 230 bars liability only if the cause of action seeks to impose liability for the provider's *publication* decisions regarding third party content—for example, whether or not to publish and whether or not to depublish. (See, e.g., *Barnes v. Yahoo!, Inc.* (9th Cir. 2009) 570 F.3d 1096 [Although taking down third-party content from its website "is quintessential publisher conduct" by a provider, Section 230 did not bar an action for promissory estoppel based on the provider's failure to remove a posting after it had agreed to do so. "Contract liability here would come not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication"]; *Hassell, supra*, 5 Cal.5th at pp. 542-543 ["we recognize that not all legal duties owed by Internet intermediaries necessarily treat them as publishers of third party content, even when these obligations are in some way associated with their publication of this material"]; *Bolger v. Amazon.com, LLC* (2020) 53 Cal.App.5th 431, 464-465 [Provider was liable in strict product

liability as a seller in the chain of distribution for a defective product. That cause of action targeted the provider's role in the distribution of consumer goods, not the third-party content in the product listing published by the provider].)

- Even if third-party content is a "but-for" cause of the harm suffered by a plaintiff, the action is not barred by Section 230 if the cause of action does not seek to hold the provider liable as a publisher. (*Internet Brands*, *supra*, 824 F.3d at p. 853 [Provider acted as a publisher of third-party content by hosting Jane Doe's user profile on a website, but the provider could be held liable for failure to warn Jane Doe based on its independent knowledge that the website was used to identify rape victims. Section 230 "does not provide a general immunity against all claims derived from third-party content" even if the third-party content was a but-for cause of plaintiff's injuries]; *HomeAway.com v. City of Santa Monica* (9th Cir. 2018) 918 F.3d 676, 682 (*HomeAway*) [Provider that hosted postings by persons offering Airbnb rentals was required to comply with an ordinance prohibiting short-term home rentals unless licensed as "home-sharing." The court rejected "use of a 'but-for' test that would provide immunity under [Section 230] solely because a cause of action would not otherwise have accrued but for the third-party content," rather looking to "whether the duty would necessarily require an internet company to monitor third-party content"]; *Lee v. Amazon.com, Inc.* (2022) 76 Cal.App.5th 200, 256 (*Lee*) [Quoting *HomeAway* and holding that a provider was required to post a warning under California's Proposition 65 where the product offered for sale by a third party on defendant's website exposed consumers to mercury].)

As discussed above, whether there is immunity for an internet service provider depends critically on the elements of the cause of action sought to be prosecuted against it. A claim is barred if it seeks to hold the provider liable as a publisher or as a speaker of third-party content.

C. Section 230 Immunity Bars Plaintiffs from Premising a Negligence Claim on Defendants' Failure to Remove CSAM and on Defendants' Failure to Create Processes to Report CSAM

Plaintiffs' allegations regarding Defendants' insufficient efforts to remove CSAM from social media sites, if true, are exceptionally concerning. For example, Plaintiffs allege that "Meta knowingly possessed the capabilities and technologies to incorporate other automatic actions into its product designs to protect children (including, but not limited to, immediately disabling or deleting harmful content to minors), but Meta deliberately and

willfully failed to do so," and that Meta "knowingly failed to invest in adequate CSAM prevention measures, including, but not limited to, client-side scanning and perceptual hashing." (Mast. Compl., ¶¶ 397-398.) As to Snap, Plaintiffs allege that it failed to use effective technologies to stop the spread of CSAM prior to Fall of 2020, that CSAM in Snap's disappearing messages cannot be reported, and that users "cannot specifically report CSAM that is sent to a user via direct messaging, including from another user's camera roll." (Mast. Compl., ¶¶ 503-507.) Plaintiffs allege that TikTok "does not have any feature to allow users to specifically report CSAM" and that "[u]sers have reported 'Post-in-Private' CSAM videos to TikTok, and ByteDance responded that no violations of its policy were found." (Mast. Compl., ¶¶ 679, 680.) As to Google, Plaintiffs allege that it "routinely fails to flag CSAM and regularly fails to adequately report known content to NCMEC and law enforcement, including CSAM depicting Plaintiffs, and fails to takedown, remove, and demonetize CSAM." (Mast. Compl., ¶ 793.) In addition, Plaintiffs allege that "there is effectively no way for users to report CSAM on Google's YouTube product." (Mast. Compl., ¶ 801.)

Nevertheless, as discussed above, a core purpose of Section 230 was to protect internet providers from liability when they deleted some offensive content from their platforms but did not delete all offensive content. (*Internet Brands*, *supra*, 824 F.3d at pp. 851-852.) Although it may seem, in retrospect, unwise to "remove disincentives for the development and utilization of blocking and filtering technologies" (47 U.S.C. § 230, subd. (b)(4)) for inappropriate and even criminally sanctionable online material, Congress chose to immunize internet service providers from liability for the "mere act of publication—including a refusal to depublish upon demand ... ." (*Hassell*, *supra*, 5 Cal.5th at p. 541.) "Congress contemplated self-regulation, rather than regulation compelled at the sword point of tort liability." (*Barrett*, *supra*, 40 Cal.4th at p. 53.) "Thus, the immunity conferred by section 230 applies even when self-regulation is unsuccessful, or completely unattempted." (*Id.*)

Liability for failure to remove CSAM posted by third parties on providers' platforms is at the core of what the immunity provided by Section 230 was designed to preclude. In 2018, Congress added subsection (e)(5) to Section 230 to make clear that the statute does not bar claims of violation of the federal sex trafficking law (18 U.S.C. §1591) or bar certain defined criminal prosecutions for sex trafficking under state law. (See generally *In re Facebook, Inc.* (Tex. 2021) 625 S.W.3d 80, 99 (*In re Facebook*).) However, Congress did not lessen internet service providers' immunity from civil liability for failure to remove abusive sexual content, even sexual content qualifying as CSAM.

Section 230 immunity from liability based on display and failure to remove third party content logically extends to Plaintiffs' allegations that Defendants failed to create adequate processes for reporting suspected CSAM. Whether the CSAM posted by a third party remains on the provider's platform because the provider had inadequate screening mechanisms, or because the provider had inadequate reporting mechanisms for CSAM makes no difference for purposes of Section 230 immunity. Both types of allegedly negligent conduct (failure to provide a mechanism to identify and remove CSAM and failure to provide a reporting mechanism for CSAM) base liability on inadequate mechanisms for removing third party content.[4]

The court grants Defendants' Motion to Strike the following paragraphs of the Master Complaint, which seek to hold the Defendants liable for failure to identify and remove CSAM and for failure to establish mechanisms for reporting CSAM: 382-384, 387-392, 394-400, 503-510, 512-513, 666-667, 679-681, 790-799, 801-802.

D. Under Current Binding Precedent, Section 230 Immunity Bars Plaintiffs from Premising a Negligence Claim on Defendants' Recommendations of Content

Defendants seek to strike portions of the Master Complaint in which Plaintiffs allege that Defendants have recommended or promoted certain content. Plaintiffs allege that TikTok recommends and promotes "challenge" videos, including those that demonstrate dangerous conduct (for example, the "Blackout Challenge" that encourages viewers to choke themselves until passing out, and the "Benadryl challenge" that encourages viewers to take large quantities of Benadryl to cause hallucinations or induce an altered mental state). (Mast. Compl., ¶¶ 608-625.) As to Google, Plaintiffs allege

[4] This court recognizes that the federal district court in the related MDL proceeding allowed a product liability claim to proceed based on "[n]ot implementing reporting protocols to allow users or visitors of defendants' platforms to report CSAM and adult predator accounts specifically without the need to create or log in to the products prior to reporting." (*In re Social Media Adolescent Addiction/Personal Injury Products Liability Litigation* (N.D. Cal., Nov. 14, 2023, No. 4:22-MD-03047-YGR) 2023 WL 7524912, at *12 (*Social Media MDL*).) The court in that decision faulted defendants for "not address[ing] how altering the ways in which they allow users and visitors to their platforms to report CSAM is barred by Section 230." (*Id.* at *13.) The court therefore allowed a product defect claim to go forward based on the allegation of inadequate reporting protocols, noting that receiving reports of suspected CSAM does not require internet service providers to remove content. (*Id.*) This court agrees with the MDL court that having an effective mechanism for reporting CSAM does not, in and of itself, require removal of CSAM. Nevertheless, in this court's view, premising liability on failure to provide an adequate reporting mechanism for CSAM targets the Defendants' actions that are part of its decision-making processes as to what content to target for removal and what content to allow to remain on their platforms, thus running afoul of Section 230's immunity for publication of third-party content.

that it also "promotes the creation of and pushes children toward extremely dangerous prank or 'challenge' videos." (Mast. Compl., ¶ 767.) Google also allegedly recommends videos of children in underwear or bathing suits, teen models, and children doing gymnastics to adults who are child predators. (Mast. Compl., ¶¶ 784-789.)

The challenge videos and videos of children are content created by the users of Defendants' platforms. As discussed above, Section 230 precludes liability premised on the existence of these videos on Defendants' platforms. Plaintiffs allege that they seek to hold Defendants liable not as publishers of the videos but rather as active promoters of the third-party content appearing on their platforms. This proposed liability conflicts with binding California authority on the interpretation of Section 230. In *Wozniak v. YouTube, LLC* (2024) 100 Cal.App.5th 893 (*Wozniak*), the California Court of Appeal held that recommendations by social media platforms are "tools meant to facilitate the communication and content of others," and thus the recommendation of third-party content is immune under Section 230. (*Id.* at pp. 916-918 [holding that YouTube's recommendations of certain harmful "scam videos" were subject to Section 230 immunity].) *Wozniak* is supported by substantial authority. (See, e.g., *Dyroff v. Ultimate Software Group, Inc.* (9th Cir. 2019) 934 F.3d 1093; *Force v. Facebook, Inc.* (2d Cir. 2019) 934 F.3d 53 (*Force*); *In re Facebook*, *supra*, 625 S.W.3d 80.)

It is worth pointing out that there have been very thoughtful opinions penned by well-respected judges that criticize the conclusion that an internet service provider is treated as a "publisher" of third-party content when it affirmatively recommends third-party content to a social media user. (See separate opinions by Judge Berzon and Judge Gould in *Gonzalez v. Google LLC* (9th Cir. 2021) 2 F.4th 871 (*Gonzalez*), vacated and remanded (2023) 598 U.S. 617, and rev'd sub nom. *Twitter, Inc. v. Taamneh* (2023) 598 U.S. 471; and separate opinion of Chief Judge Katzman in *Force*, *supra*, 934 F3d at pp. 76-89.) The United States Supreme Court granted certiorari in *Gonzalez* to address this question, but ultimately did not reach the issue, essentially resolving the case on other grounds. (*Twitter, Inc. v. Taamneh* (2023) 598 U.S. 471.) Despite the persuasive reasoning of these concurring and dissenting views, this court is bound by *Wozniak.* Thus, under existing authority, Section 230's immunity bars the Plaintiffs' theory of a duty arising out of TikTok's promotion of challenge videos.

The allegations concerning Defendants' promotion of challenge videos and videos of children are not analogous to the facts in *Lemmon v. Snap, Inc.* (9th Cir. 2021) 995 F.3d 1085 (*Lemmon*). In *Lemmon,* the plaintiffs were parents of two deceased boys who sued Snap, "alleging that it encouraged their sons to drive at dangerous speeds and thus caused the

boys' deaths through its negligent design of its smartphone application Snapchat." (*Id.* at p. 1087.) At issue was Snap's app called the "Speed Filter." "The app ... permits its users to superimpose a filter over the photos or videos that they capture through Snapchat at the moment they take that photo or video. [One of the deceased boys] used one of these filters—the Speed Filter—minutes before the fatal accident on May 28, 2017. The Speed Filter enables Snapchat users to record their real-life speed." (*Id.* at p. 1088, internal quotation marks omitted.) "Many of Snapchat's users suspect, if not actually believe, that Snapchat will reward them for recording a 100-MPH or faster snap using the Speed Filter. According to plaintiffs, this is a game for Snap and many of its users with the goal being to reach 100 MPH, take a photo or video with the Speed Filter, and then share the 100-MPH-Snap on Snapchat." (*Id.* at p. 1089, internal quotation marks and brackets omitted.)

The Ninth Circuit reversed the district court's dismissal of the plaintiffs' action under Section 230, concluding "that, because the [plaintiffs'] claim neither treats Snap as a publisher or speaker nor relies on information provided by another information content provider, Snap does not enjoy immunity from this suit under § 230(c)(1)." (*Id.* at p. 1087, internal quotation marks omitted.) The court noted that the plaintiffs in *Lemmon* alleged a cause of action that "rest[ed] on the premise that manufacturers have a duty to exercise due care in supplying products that do not present an unreasonable risk of injury or harm to the public." (*Id.* at p. 1092.) The court then concluded that the claims were not barred by Section 230:

> The duty underlying such a claim differs markedly from the duties of publishers as defined in [Section 230]. Manufacturers have a specific duty to refrain from designing a product that poses an unreasonable risk of injury or harm to consumers. [Citation.] Meanwhile, entities acting solely as publishers—*i.e.*, those that "review material submitted for publication, perhaps edit it for style or technical fluency, and then decide whether to publish it," [citation]—generally have no similar duty. [Citation.]
>
> It is thus apparent that the [plaintiffs'] amended complaint does not seek to hold Snap liable for its conduct as a publisher or speaker ... . [T]he duty that Snap allegedly violated "springs from" its distinct capacity as a product designer. [Citation.] This is further evidenced by the fact that Snap could have satisfied its "alleged obligation"—to take reasonable measures to design a product more useful than it was foreseeably dangerous—without altering the content that Snapchat's users generate. [Citation.] Snap's

> alleged duty in this case thus "has nothing to do with" its editing, monitoring, or removing of the content that its users generate through Snapchat. [Citation.]

(*Id.*, internal citations and brackets omitted; italics in original.)

Unlike the allegations here, the facts in *Lemmon* were that the Speed Filter *itself* encouraged users to engage in dangerous driving; here, by contrast, it is the specific third-party content presented in the challenge videos and videos of children and the recommendation of the content that give rise to the injuries alleged. The court in *Wozniak* rejected reliance on *Lemmon* for the same reasons. (*Wozniak*, *supra*, 100 Cal.App.5th at p. 913.) As stated above, under current California law interpreting Section 230, liability based on promotion of challenge videos is barred.[5]

The court therefore grants Defendants' Motion to Strike the following paragraphs of the Master Complaint, which seek to hold Defendants liable for recommending dangerous content to minors: 365-368, 372 (allegations as to Instagram), 608-625, 767, 784-789. The court also strikes the language Defendants challenge in the J.S. SFC.

E. Plaintiffs' Claims Premised on Affirmative Acts that Increase Risk of Harm to Minors from Sexual Exploitation by Third Parties

Plaintiffs allege that a number of affirmative actions of Defendants regarding design of their social media platforms and communication with the minor Plaintiffs foreseeably increased the risk that Plaintiffs would be sexually exploited by other users of the platforms. Plaintiffs' allegations, which the court must accept as true at this point, describe an ecosystem created by Defendants that increase the likelihood that a sexual predator can find, contact, groom, and solicit sexually explicit material from minors. Plaintiffs seek to hold Defendants liable for the following conduct:

- Creating a geolocation feature that allows strangers access to data by which minors can be located.
- Affirmatively recommending that minors contact strangers.
- Creating systems to allow strangers to send cash to minors and to reward them with "virtual gifts."
- Encrypting direct messages between minors and strangers.
- Creating a means by which users can make images they create or see disappear.

[5] Because the court finds that Plaintiffs' claims based on online challenge videos are barred by Section 230, the court does not reach Defendants' argument that allegations of injury from online challenges are independently barred by the First Amendment.

- Inadequate mechanisms for age verification.
- Setting minors' accounts to "public" as a default.

*1. Plaintiffs Have Adequately Alleged a Claim for Negligence Based on Defendants' Affirmative Conduct that Allegedly Increases the Risk of Injury to the Minor Plaintiffs*

Before determining whether Section 230 applies, this court must first determine whether these allegations can properly underlie a claim for negligence under the common law. Defendants argue that, in order to state a negligence claim based on Defendants' conduct that allegedly connected minor users of Defendants' social media sites with adults who sexually abused the minors, Plaintiffs must allege that Defendants have a "special relationship" with minor users of Defendants' platforms. However, under California law, a defendant is liable for its affirmative conduct that increases the risk of injury to another from the foreseeable conduct of a third party. As discussed below, Plaintiffs' allegations of affirmative conduct by Defendants that increased the risk the minor plaintiffs would be sexually abused by an adult adequately state a claim for relief under California law.

"[T]he law imposes a general duty of care on a defendant only when it is the defendant who has created a risk of harm to the plaintiff, including when the defendant is responsible for making the plaintiff's position worse." (*Brown v. USA Taekwondo* (2021) 11 Cal.5th 204, 214, internal citations and quotation marks omitted.) "This general rule ... derives from the common law's distinction between misfeasance and nonfeasance, and its reluctance to impose liability for the latter." (*Id.*, internal citations and quotation marks omitted.) Stated more precisely, "[t]he proper question is not whether an actor's failure to exercise reasonable care entails the commission or omission of a specific act. [Citation.] Rather, it is whether the actor's entire conduct created a risk of harm." (*Id.*, at p. 215, fn. 6, internal citations and quotation marks omitted, citing Rest.3d Torts, Liab. for Phys. & Emot. Harm (2012) § 37, com. c, p. 3.)

As stated in Section 19 of the Restatement Third of Torts, Liability for Physical and Emotional Harm: "The conduct of a defendant can lack reasonable care insofar as it foreseeably combines with or permits the improper conduct of the plaintiff or a third party." Regarding the scope of an actor's liability for actions that increase the risk of third-party misconduct, the Restatement notes that "[i]f the third party's misconduct is among the risks making the defendant's conduct negligent, then ordinarily plaintiff's harm will be within the defendant's scope of liability." (Rest.3d Torts, Liab. for Phys. & Emot. Harm, § 19, com. c.) Thus, when the actor has sufficient knowledge of the circumstances to foresee criminal misconduct by a third

party, negligence liability may be imposed for the actor's conduct that increases the risk of harm to another by a third party. (*Id.* com. f.)

In *Weirun v. RKO General, Inc.* (1975) 15 Cal.3d 40, the California Supreme Court, in a decision written by Justice Stanley Mosk, held that a radio broadcast had created an unreasonable risk of harm to its listeners by encouraging their participation in a contest involving a race on city streets to obtain cash prizes. (*Id.* at p. 47.) The Supreme Court found the radio station liable to a listener who was killed in a car crash while pursuing the contest prize money. The Supreme Court stated that it was "of no consequence that the harm to decedent was inflicted by third parties acting negligently" because of "the likelihood that a third person may react in a particular manner is a hazard which makes the actor negligent ... ." (*Id.* at p. 47.) "Liability is imposed only if the risk of harm resulting from the [defendant's] act is deemed unreasonable—i.e., if the gravity and likelihood of the danger outweigh the utility of the conduct involved." (*Id.*, citing Prosser, Law of Torts (4th ed. 1971) at pp. 146-149.)

In *Lugtu v. California Highway Patrol* (2001) 26 Cal.4th 703, the California Supreme Court held that a law enforcement officer could be held liable in negligence for having pulled over the plaintiff's automobile into the center median strip of a highway where it was struck by another vehicle, injuring plaintiff. The court stated: "It is well established ... that one's general duty to exercise due care includes the duty not to place another person in a situation in which the other person is exposed to an unreasonable risk of harm through the reasonably foreseeable conduct ... of a third person." (*Id.* at p. 716.)

The standard of duty is heightened because the affirmative conduct allegedly engaged in by Defendants was conduct involving a minor. For example, the foreseeable consequences of Defendants' creation of a geolocation feature may be different for a minor user—who may be unable to appreciate the danger that others may try to locate the minor for harmful purposes—than it would be for an adult user. The legal standard of duty when interacting with minors is that "[a]n adult must anticipate the ordinary behavior of children. An adult must be more careful when dealing with children than with other adults." (CACI No. 412.)

In *McDaniel v. Sunset Manor Co.* (1990) 220 Cal.App.3d 1, the court of appeal held that "[a] greater degree of care is generally owed to children because of their lack of capacity to appreciate risks and to avoid danger. ... The determination of the scope of foreseeable perils to children must take into consideration the known propensity of children to intermeddle." (*Id.* at p. 7.) In that case, the court held that, because the defendant landowner

had built a fence around its property but had allowed the fence to become dilapidated (to develop holes), there was an issue of fact as to whether the landowner was liable for injury to a child who entered through a hole in the fence and then fell into a creek on adjacent property from a vertical drop of at least seven feet. (*Id.* at pp. 4, 8-10.)

Plaintiffs have adequately pleaded that Defendants affirmatively developed and implemented features on their social media platforms that created dangerous conditions for minors by increasing the risk that vulnerable minors would be identified and sexually preyed upon by adult strangers. For purposes of California pleading standards, Plaintiffs have adequately alleged that the identified features materially contributed to the danger that minors would encounter and be injured by adult strangers on Defendants' social media platforms. (See CACI No. 430 ["A substantial factor in causing harm is a factor that a reasonable person would consider to have contributed to the harm. It must be more than a remote or trivial factor. It does not have to be the only cause of the harm"].)

*2. Whether Liability for Affirmative Acts of Defendant Alleged to Have Increased the Risk of Injury to Minors Is Barred by Section 230*

a. Geolocation of Minors

Defendants assert that binding California precedent bars a claim for liability based on any choice an interactive computer service provider makes in designing a social media platform. (See Defs' Mot., at pp. 16-17.) In support of this assertion, Defendants principally rely on *Doe II v. MySpace, Inc.* (2009) 175 Cal.App.4th 561 (*MySpace*). Although *MySpace* recognizes and applies Section 230's broad grant of immunity, the case does not sweep as broadly as Defendants contend. As the panel in that case recognized, Section 230 does not bar liability for an interactive computer service provider's own decisions as a content developer.

In *MySpace*, the complaint sought recovery for injuries suffered by minor users of a social media platform, MySpace, who were sexually assaulted by men they met through interactions on the platform. (*Id.* at p. 564.) The plaintiffs "characterized their complaint as one for failure to adopt reasonable safety measures" and the court viewed the claims of plaintiffs, at their core, as seeking to regulate what appears on the social media platform. (*Id.* at p. 573.)

The *MySpace* court distinguished the facts before it from the circumstances considered in *Roommates.* In *Roommates*, the Ninth Circuit Court of Appeals held that Section 230 did not bar liability where the

provider "designed its search and email systems to limit the listings available to subscribers based on sex, sexual orientation and the presence of children" and thereby allegedly engaged in unlawful discriminatory conduct. (*Roommates, supra,* 521 F.3d at p. 1169.) In *MySpace*, the court construed *Roommates* as involving "two ends of the spectrum with respect to how much discretion a third party user has in the content he or she posts on the site." (*MySpace*, at p. 575.) In *Roommates*, a subscriber was required to select one answer from a limited number of choices in the profile section but was given unfettered discretion as to content in the "additional comments" section; the provider could be held responsible for the former but not for the latter. (*Id.*) The *MySpace* court characterized the MySpace website at issue as providing "neutral tools" from which users could create their profile. The court found it dispositive that MySpace did not "require[ ] its members to answer the profile questions as a condition of using the site." (*Id.*) Based on that characterization, the *MySpace* court held that the plaintiffs' claims for liability were based on third-party content published by the plaintiffs themselves, not on the actions of the website provider.

One of the choices some Defendants have made in designing their platforms is to provide a location feature that tracks individual platform users and allows them to "geotag the location where a photo was taken or from where a post is being made." (Mast. Compl., ¶ 380 as to Meta; see Mast. Compl., ¶ 669 as to ByteDance.) This feature does not ask the user to identify the place where the user was located when the user made a post or took a photograph and then publish the information provided by the user. If the user voluntarily placed such information on the social media site and a third party was thereby enabled to find that user, Section 230 would protect the provider from liability derived from content provided by the user. The geolocation feature, however, provides location content both created and published by the internet service provider. The geolocation tag is derived not from information furnished by the user but rather from the Defendants' decision to track the location of the user's cell phone and then to publish this provider-created content.

Under Section 230, the provider is not "treated as the publisher or speaker of any information provided by another information content provider" if a Defendant is found to have increased the risk of sexual abuse of a plaintiff by having developed and published the geotag information. Rather, Plaintiffs seek to hold Defendants liable for tracking a user to develop and publish location information identifying where a Plaintiff is when he or she posts a message or a photo. Plaintiffs' theory of liability based on the increased risk for minors due to Defendants' geolocation features is not barred by Section 230.

Defendants argue that cases from other jurisdictions have held that Section 230 bars liability for harm caused by information provided by an internet service provider's geolocation device. But neither case cited by Defendants actually concerns liability based on a geolocation device provided by a social media company. In *Herrick v. Grindr LLC* (2d Cir. 2019) 765 F.App'x 586 (*Herrick*), the plaintiff sought to hold the defendant social media provider liable because of harm caused by her boyfriend's posts that impersonated her and directed other users to her home and workplace. (*Id.* at p. 588.) The plaintiff in that case contended that the geolocation device provided by the social media website was used to direct other users to her home and workplace. The court of appeal held that Section 230 barred liability because the defendant's geolocation device *was not in fact used* to direct users to plaintiff's location. It was "uncontested that [plaintiff] was no longer a user of the app at the time the harassment began; accordingly, any location information was necessarily *provided by [plaintiff's] ex-boyfriend.*" (*Id.* at p. 590, emphasis added.) Thus, the defendant website could not be held liable based on content provided by the ex-boyfriend.

Neither are the facts of *Marshall's Locksmith Service Inc. v. Google, LLC* (D.C. Cir. 2019) 925 F.3d 1263 (*Marshall's*) analogous to the facts alleged here. In that case, the plaintiffs were locksmith companies that alleged the defendant social media providers flooded the market with online search results about "scam" locksmiths. The plaintiffs based their contentions in part on defendants' publication of maps with pinpoints on where the scam locksmiths could be found. The court of appeal held that Section 230 barred the plaintiffs' claims based on the maps because the maps were created using street addresses and locations that were copied by the defendants from the scam locksmiths' own representations in their webpages. The court of appeal held that Section 230 protection applied when the pinpoints on the maps only translated address information provided by the third-party scam locksmiths into map form. (*Id.* at p. 1270.) When the pinpoints on the maps were created by a "neutral algorithm" that translated approximate location information provided by the scam locksmith into a map format, the same result obtained because, again, the location information expressed in the map was content provided by a third party.

Here, the geolocation information was created by Defendants by tracking the minors' cell phones. Unlike the circumstances in *Herrick* and *Marshall's*, the minors here did not provide the location information—it was based on the Defendants' tracking function. Liability therefore is not premised on publication of third-party content, and Section 230 does not bar Plaintiffs' claims that Defendants' provision of a geolocation device to track

minors and publish their locations is negligent because it increases the risk that Plaintiffs will be victims of predatory conduct.

As in *Lemmon*, the geolocation feature for which Plaintiffs seek to hold Defendants liable "has nothing to do with [Defendants'] editing, monitoring, or removing the content that its users generate using" the social media site." (*Lemmon*, *supra*, 995 F.3d at p. 1092, internal quotation marks omitted.) In *Lemmon*, the social media defendant applied a notation to a photograph taken by the user; the notation was created by a "Speed Filter" the provider created by tracking the speed at which the user was traveling at the time the photo was taken. Here, Defendants apply a notation to a photograph taken by the user or content posted by the user; the notation is created by a geolocation device the Defendants' created to track the location of the user at the time the photo was taken or the posting was made. By analogy to *Lemmon*, Section 230 does not bar liability based on Plaintiffs' claim that Defendants' decision to create a location-tracking capability and to apply a location notation to minors users' content increased the risk of harm to the minors from third-party conduct.

The court therefore denies Defendants' Motion to Strike the following paragraphs of the Master Complaint alleging liability flowing from Defendants' use of geolocation features: 380-381, 669.

b. Recommending "Friends" for Minors

Plaintiffs allege that Facebook uses algorithms "to suggest users for 'friending' to each other" and "Facebook does not provide the option to disable this feature." (Mast. Compl., ¶ 172.) According to the Master Complaint, "Facebook's 'People You May Know' feature helps predators connect with underage users and puts them at risk of sexual exploitation, sextortion, and production and distribution of CSAM; 80% of 'violating adult/minor connections' on Facebook were the result of this friends recommendation system." (Mast. Compl., ¶ 372.) As to Snap, Plaintiffs allege:

> Through a feature known as "Quick Add," Snap recommends new, sometimes random friends, similar to Facebook's "People You Might Know" feature. Suggestions are formulated using an algorithm that considers users' friends, interests, and location. Quick Add encourages users to expand their friend base to increase their Snapscore by interacting with an ever-expanding group of friends, which ... can result in exposure to dangerous strangers ... . Quick Add

> could, and in fact did, recommend that a minor and adult user connect.

(Mast. Compl., ¶481.) As to TikTok, Plaintiffs allege that the platform "intentionally and actively promoted" connections between children and strangers 'by suggesting accounts to follow through the 'Find Friends' or 'People You May Know' features." (Mast. Compl., ¶ 555.)

Under the reasoning of *MySpace*, Section 230 does not bar liability for Defendants' decisions to employ a feature that recommends a personal contact to a minor. As explained above, *MySpace* interpreted the plaintiffs' claims in that case as seeking to regulate what third parties post on a social media platform. (*MySpace*, *supra*, 175 Cal.App.4th at p. 573.) Under the facts alleged in that case, users created profiles on topics suggested by the social media provider and "[o]ther MySpace users are then able to search and view profiles that fulfill specific criteria ... ." (*Id.* at p. 564.) As described by the court of appeals, "MySpace channels information based on members' answers to various questions, allows members to search only the profiles of members with comparable preferences, and sends e-mail notifications to its members." (*Id.*) The contacts for which the plaintiffs in *MySpace* sought to hold the social media provider liable were contacts that were (1) based on information provided by the user (third-party content), and (2) based on searches performed by the user.

Here, by contrast, Plaintiffs do not seek to hold Defendants liable for information posted by third-party users or for the results of searches made possible by Defendants but performed by users. Instead, Plaintiffs allege that Defendants' own affirmative acts increased the risk of harm to the minors because of Defendants' own speech, unprompted by a request from the user, that recommended that the minor pursue a contact with an identified person. The court of appeals in *MySpace* had no reason to consider, and did not analyze, the scope of Section 230 protection of an internet service provider when the provider's own speech was the asserted basis for liability. Moreover, the *MySpace* court's discussion of *Roommates* acknowledged that a social media provider may be chargeable with liability based on the provider's own speech or creation of content, and that Section 230 does not bar liability in those circumstances.

Defendants' recommendations of "friends" for minor users also cannot be characterized as the publication of third-party content. In *Wozniak*, the court of appeal held that the defendants' recommendation of scam videos "does not make them information content providers because those recommendations did not materially contribute to the illegality of the content underlying the scam." (*Wozniak*, *supra*, 100 Cal.App.5th at p. 921.)

However, the court left open the possibility that liability would not be barred by Section 230 if based on the social media providers' actions in "continu[ing] to maintain the verification of channels that have been hijacked to broadcast ... scam videos ... ." (*Id.* at p. 924, internal quotation marks omitted.) The court of appeals concluded that the complaint "adequately alleges that under section 230 [defendant] is responsible for creating the information in the verification badges." (*Id.* at p. 924.) The court held that, so long as the plaintiffs amended to allege "that the information for which defendants are responsible gives rise to their asserted liability or materially contributed to the illegality of the conduct at issue," Section 230 would not bar such claim. (*Id.*) Thus, despite *Wozniak*'s determination that providers cannot be held liable for recommending content, the court recognized that Section 230 does not immunize a provider's speech or conduct that characterizes third party content as authentic.

As stated in *Liapes*, "providing neutral tools to users to make illegal or unlawful searches does not constitute development for immunity purposes. But the system must do absolutely nothing to enhance the unlawful message at issue beyond the words offered by the user." (*Liapes*, *supra*, 95 Cal.App.5th at p. 930.) Here, Plaintiffs' allegations are not merely that Defendants recommended third-party content to a minor, but that Defendants referred to the person posting the content as a "friend" or someone the minor "might know." This label and recommendation allegedly enhanced the danger posed to a minor user beyond the danger posed by the mere existence of a fraudulent user profile somewhere on the social media site. Liability is alleged to be based not on the third-party content of a fraudulent profile (e.g., a profile of a 40-year-old man pretending to be 15 years old), and not for recommending content contained in the fraudulent profile, but for affirmatively recommending the creator of the profile as a "friend" with whom a minor (who has not searched for any content or contact) should establish an online relationship. Because Defendants enhanced the fraudulent message, they may be held liable for increasing the risk to Plaintiffs' use of Defendants' social media platforms. Again, as in *Lemmon*, the allegations here target the conduct of Defendants in creating a feature that increases the danger to Plaintiffs, not because of content posted on the website, but because the feature seeks to engage the minor Plaintiffs in dangerous activity (contact with strangers, especially adult strangers).

In *A.M. v. Omegle.com, LLC* (D.Or. 2022) 614 F.Supp.3d 814, the federal district court reached similar conclusions. In that case, the plaintiff brought a products liability claim against an internet service provider for randomly pairing a minor Plaintiff with an adult man for one-on-one chats. Ultimately, the plaintiff was sexually abused online through the defendant's

social media platform. (Id. at p. 817.) The district court held that Section 230 did not bar this claim for two reasons. First, the plaintiff's theory of liability did not require that the defendant "review, edit or withdraw any third-party content," but rather was premised on an allegedly dangerous product design feature created by the defendant (randomly matching people for one-on-one chats). (*Id.* at p. 819.) Second, liability was not imposed based on holding the defendant responsible for the adult abuser's communications to the plaintiff, but rather was imposed based on the product that was designed "in a way that connects individuals who should not be connected (minor children and adult men) and that it does so before any content is exchanged between them." (*Id.* at pp. 820-821.)

The court therefore denies Defendants' Motion to Strike as to the following paragraphs of the Master Complaint alleging liability based on Defendants' recommendation of contacts to minors: 172, 372, 481-483, and 555. Because Defendants have failed to demonstrate that there is no actionable conduct by Defendants on which Plaintiffs' claims for exploitation and/or sexual abuse related harms may be based, the court also denies the Motion to Strike as to the A.S. SFC, Glen-Mills SFC, K.L. SFC, N.S. SFC, P.F. SFC and K.K. SFC.

c. Money and Virtual Gifts

Plaintiffs allege that Defendants increased the risk of harm to minor Plaintiffs from online sexual predators by creating features that allow the predators to send money or gifts to minors through the social media site, and to communicate privately by voice or video call through the website. From 2014 to 2018, Snapchat included a feature known as "Snapcash," which was a "peer-to-peer mobile payment service." Snapcash allegedly "provided a way for users to pay for private content with little to no oversight" and "enabled predators to extort cash from adolescent users by threatening to disseminate CSAM to other users." (Mast. Compl., ¶ 499.) A feature of Snapchat "allows users to voice or video call one another in the app." (Mast. Compl., ¶ 501.) This feature allegedly "allows predators to call and video chat with minors in private, with virtually no evidence of what was exchanged." (Mast. Compl., ¶ 501.) "ByteDance's design of the 'LIVE Gifts' and 'Diamonds' rewards allegedly greatly increases the risk of adult predators targeting adolescent users for sexual exploitation, sextortion, and CSAM." (Mast. Compl., ¶ 677.)

None of these features involves publication of third-party content. Rather they are modalities for payment of money or provision of virtual rewards that allegedly are significant to minors, or they are instruments for verbal communication. These features are designed by Defendants and

cannot be analogized to functions of publishers or distributors of third-party content. They are not rewards for publishing content; they are means for users to pay or favor one another or to have verbal contact.

Defendants assert that the "gravamen" of these allegations is injury caused by content on the social media services. (Defs' Supp. Br., at p. 12.) This is an incorrect reading of the allegations. The gravamen of Plaintiffs' claims based on these features is that Defendants' affirmative acts increased the risk of harmful third-party conduct toward the minor Plaintiffs. Plaintiffs contend that these payments and verbal communication modalities increase minors' risk of harm from sexual predators. In some instances, the rewards or verbal communications are alleged to lead to in-person contact between the minor and the sexual predator. In other instances, the rewards or verbal communications are alleged to be part of a sextortion scheme that occurs partly online. In the latter instance, even if third-party content is a "but-for" cause of the harm suffered by a plaintiff, the action is not barred by Section 230 because the cause of action does not seek to hold the provider liable as a publisher. (See *Internet Brands*, *supra*, 824 F.3d at p. 853 [Section 230 "does not provide a general immunity against all claims derived from third-party content" even if the third-party content was a but-for cause of plaintiff's injuries]; *HomeAway*, *supra*, 918 F.3d at p. 682; *Lee*, *supra*, 76 Cal.App.5th at p. 256.)

Defendants also cite *Wozniak* for the proposition that a claim against a provider may not be based on "sale of advertisements" when liability is "ultimately predicated on the third party content." (Defs' Supp. Br., at p. 12, citing *Wozniak*, *supra*, 100 Cal.App.5th at p. 915.) *Wozniak* is inapposite. In that case, there was no allegation that the defendants themselves created the advertisements, and the injury was alleged to flow not from selling advertisements to third parties but from publishing the third parties' advertising of their scam videos. There, the plaintiffs "object[ed] to the content of the advertisements themselves, which promote[d] the scam." (*Wozniak*, at p. 915.) In contrast, here, the features created by Defendants that allegedly increased the risk of harm were not based on content provided by third parties; rather, they served as a modality separate from published content that allowed adult predators to influence minors while eluding detection.[6]

---

[6] Defendants also cite *La Park La Brea A LLC v. Airbnb, Inc.* (C.D. Cal. 2017) 285 F.Supp.3d 1097, 1106, for the proposition that the processing or receipt of payments associated with posts does not strip a provider of immunity under section 230. But nothing in that case changes the correct analysis under Section 230: determining whether liability is premised on a provider's publication decision regarding third-party content. Here, the rewards and money payments are alleged to independently create a risk for minors regardless of Defendants' publication decisions concerning third-party content.

The court denies Defendants' Motion to Strike the following paragraphs of the Master Complaint alleging liability based on Defendants' social media site features that allow minors to receive money or gifts through the site: 499 and 677.

d. Private Direct Messaging and Private Posting or Communication of Images

Defendants seek to strike portions of the Master Complaint in which Plaintiffs allege they are injured by Defendants' decisions to allow users to exchange private messages or videos (Mast. Compl., ¶¶ 377, 385 as to Meta; ¶¶ 673-674, 678 as to ByteDance), to limit display time for images (Mast. Compl., ¶¶ 472-473 as to Snap) and to allow content to be hidden in a tab that requires a passcode and will self-destruct if a user attempts access with the wrong code (Mast. Compl., ¶¶ 476-477).

While these features are allegedly dangerous for minors, they in fact are Defendants' decisions about how to publish and disseminate content; therefore, liability may not be premised on Defendants' decisions to allow users to publish content that is ephemeral or hidden from others. Unlike the features discussed above, these features embody decisions about how to publish content. (See *Batzel, supra*, 333 F.3d at p. 1031 ["the exclusion of 'publisher' liability necessarily precludes liability for exercising the usual prerogative of publishers to choose among proffered material and to edit the material published while retaining its basic form and message"].) Defendants have chosen to publish material that the information content providers wanted to remain private to various extents; this is a decision that is protected by Section 230 immunity.

This court agrees with the conclusions reached in *LW through Doe v. Snap Inc.* (S.D. Cal. 2023) 675 F.Supp.3d 1087. In that case, several plaintiffs alleged that when they were minors they were contacted on social media (not on the platform of the defendant in that case) by a sexual predator and then began communicating with the predator on Snapchat, facilitated by Snapchat's ephemeral design features, specifically the disappearing messages. The federal district court found that the "harm animating Plaintiffs' claims is directly related to the posting of third-party content on [Snapchat]." (*Id.* at p. 1097, internal citations and quotation marks omitted.) "Plaintiffs' arguments more closely implicate a publication function than a design or development function." (*Id.*)

Although this court finds that liability may not be premised on Defendants' practices of publishing ephemeral or private content, the court

will not strike from the Master Complaint all reference to the existence of, and user access to, ephemeral or private content. These allegations serve as background facts that support Plaintiffs' allegations that other actionable conduct of Defendants is negligent. For example, the fact that a minor may communicate using ephemeral content and may have secret messaging with a third party reflects on the reasonableness of Defendants' conduct in introducing minors to "friends" who are adults the minors do not know. (See Mast. Compl., ¶ 377 [explaining how exchange of private direct messaging makes predatory conduct more likely after a minor has received a message from a stranger].) Plaintiffs also have alleged that Defendants have designed their platforms with inadequate parental controls, and Defendants have not sought to strike these allegations. (See, e.g., Mast. Compl., ¶¶ 259, 261, 401 as to Meta; ¶¶ 491-493 as to Snap; ¶¶ 540, 659 as to ByteDance.)[7] The factual contentions concerning Snapchat's "My Eyes Only" feature (Mast. Compl., ¶¶ 476-477), which Defendants seeks to strike, may serve as background for understanding why Snap's "Family Center" feature for parental control (Mast Compl., ¶ 493), which Defendants do not seek to strike, is allegedly inadequate.

A motion to strike is proper to remove irrelevant matter from a complaint. (Code Civ. Proc., § 436, subd. (a).) Irrelevant matter includes allegations "neither pertinent to nor supported by an otherwise sufficient claim or defense." (Cal. Prac. Guide Civ. Pro. Before Trial (The Rutter Group) Ch. 7(I), ¶ 7:178-B, quoting Code Civ. Proc., § 431.10, subd. (b)(2).) Because the Master Complaint's allegations concerning private direct messaging and private videos, even though not actionable in themselves, are relevant to Plaintiffs' actionable claims regarding the potential dangers from the "friends" features, and are relevant to evaluation of Defendants' allegedly negligent conduct in crafting parental controls, the allegations concerning private direct messaging and private videos are not irrelevant matter.[8]

The court therefore denies Defendants' Motion to Strike the following paragraphs of the Master Complaint which describe Defendants' publication features that allow private communication and/or private posting of information: 377-378, 385, 472-473, 476-477, 497-498, 501-502, 670, 673-674 and 678.

---

[7] This court notes that the MDL court allowed the plaintiffs there to assert negligence claims based on Defendants' allegedly ineffective parental controls. (*Social Media MDL*, *supra*, 2023 WL 7524912, at *12.)

[8] It is premature for the court to address whether a limiting instruction would be appropriate if evidence concerning, for example, private direct messaging is introduced at trial.

e. Lack of Age Verification and Default Public Setting for Minors' Profiles

Plaintiffs allege that the "absence of effective age verification measures ... allows predators to lie about their ages and masquerade as children, with obvious dangers to the actual children on Meta's products." (Mast. Compl., ¶ 373.) Plaintiffs also allege that minors' user profiles are allowed to be publicly viewable by any user as a default setting, allowing strangers to contact minor users. (Mast. Compl., ¶¶ 374, 555.) Defendants seek to strike these allegations, arguing that claims of liability based on them are barred by Section 230 immunity.

Claims based on Defendants' failure to implement effective age verification software and on implementing a default public setting for user profiles are barred by *MySpace.* (*MySpace*, *supra*, 175 Cal.App.4th at p. 565 [barring plaintiffs' claims based on allegations "that MySpace should have implemented readily available and practicable age-verification software or set the default security setting on the [plaintiffs'] accounts to private"], internal quotation marks omitted.) However, as is the case with Plaintiffs' allegations concerning direct messaging and private videos, the facts pleaded concerning a lack of age verification and the default public setting are not irrelevant matter because they may be admissible to explain the potential dangers from the "friends" features and why parental controls are allegedly inadequate to protect minors from other dangers, including addiction to Defendants' platforms. Although Section 230 precludes liability for the absence of age verification and the decision to make minors' profiles public, the fact that these features exist is not irrelevant matter because it allegedly explains in part why other actions by Defendants were negligent.

For the foregoing reasons, the court denies Defendants' Motion to Strike the following paragraphs of the Master Complaint which describe Defendants' age verification and default public setting for minor profiles: 373-374, 494-495, 550, and 556.

## III. CONCLUSION

Defendants' Motion to Strike is granted in part, denied in part, and denied without prejudice in part as specified in the foregoing decision.

Defendants also seek to strike certain words, sentence fragments and sentences from other paragraphs of the Master Complaint as set forth in items 9 through 39 of the Motion to Strike. Because this court has addressed all substantive issues raised by the Motion to Strike, the court orders the parties to meet and confer to reach agreement as to how this

court's opinion should be applied to items 9 through 39. As to any item on which there is disagreement, the parties shall file a brief joint report setting forth their respective positions. Insofar as the parties agree how this court's rulings affect the sentences and fragments listed in items 9 through 39, the parties shall file a stipulated proposed order granting or denying the Motion to Strike those items (but preserving the parties' respective positions as stated in the briefing of the Motion to Strike).

**IT IS SO ORDERED**

July 19, 2024

Carolyn B. Kuhl
Judge of the Superior Court