APPENDIX TABLE OF CONTENTS

OPINIONS AND ORDERS

REHEARING ORDERS

STATUTORY PROVISIONS

OTHER DOCUMENTS

OPINION, U.S COURT OF APPEALS FOR THE NINTH CIRCUIT (AUGUST 22, 2024)

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

THE ESTATE OF CARSON BRIDE, by and through his appointed administrator KRISTIN BRIDE; A.K., by and through her legal guardian Jane Doe 1; A.C., by and through her legal guardian Jane Doe 2; A.O., by and through her legal guardian Jane Does 3; TYLER CLEMENTI FOUNDATION, on behalf of themselves and all others similarly situated,

Plaintiffs-Appellants,

v.

YOLO TECHNOLOGIES, INC.,

Defendant-Appellee.

No. 23-55134

D.C. No. 2:21-cv-06680-FWS-MRW

Appeal from the United States District Court
for the Central District of California
Fred W. Slaughter, District Judge, Presiding

Argued and Submitted April 11, 2024
Pasadena, California

Filed August 22, 2024

Before: Eugene E. SILER,* Carlos T. BEA, and Sandra S. IKUTA, Circuit Judges.

OPINION

SILER, Circuit Judge:

Appellee YOLO Technologies developed an extension for use on the Snapchat application ("app") which allowed users to ask public questions and send and receive anonymous responses. YOLO informed all users that it would reveal the identities of, and ban, anyone who engaged in bullying or harassing behavior. Appellants, three living minor children and the estate of a fourth, all suffered extreme harassment and bullying through YOLO resulting in acute emotional distress, and in the case of Carson Bride, death by suicide. They brought this diversity class action alleging that YOLO violated multiple state tort and product liability laws by developing an anonymous messaging app which promised to unmask, and thereby prevent, bullying and abusive users, but YOLO never actually did so.

The district court held that § 230 of the Communications Decency Act immunized YOLO from these claims and dismissed the complaint. We affirm and reverse in part, holding that § 230 bars Plaintiffs' products liability claims but not their misrepresentation claims.

---

* The Honorable Eugene E. Siler, United States Circuit Judge for the U.S. Court of Appeals for the Sixth Circuit, sitting by designation.

I.

A.

YOLO Technologies developed their app as an extension upon the already-popular Snapchat app. Marketed mainly toward teenagers in mobile app stores, YOLO achieved tremendous popularity, reaching the top of the download charts within a week of its launch. It eventually reached ten million active users.

Anonymity was YOLO's key feature. Users would install the app and use it to post public questions and polls for their followers. Other users, also using YOLO, could respond to the questions or polls anonymously, unless they chose to "swipe up" and voluntarily disclose their identity as part of their answer. Without such voluntary revelation, the recipient would not know the responder's account nickname, user information, or any other identifying data.

Anonymous messaging applications, even ones marketed specifically to teens, are not new inventions. Plaintiffs contend that "it [has] long been understood that anonymous online communications pose a significant danger to minors, including by increasing the risk of bullying and other antinormative behavior." In fact, prior applications with anonymous communication features had caused "teenagers [to] take[] their own lives after being cyberbullied."

As a hedge against these potential problems, YOLO added two "statements" to its application: a notification to new users promising that they would be "banned for any inappropriate usage," and another promising to unmask the identity of any user who "sen[t] harassing messages" to others. But, Plaintiffs

argue, with a staff of no more than ten people, there was no way YOLO could monitor the traffic of ten million active daily users to make good on its promise, and it in fact never did. Many user reviews of the YOLO app on Apple's app store reflected frustration with harassing and bullying behavior.

B.

Plaintiffs A.K., A.C., A.O., and Carson Bride all downloaded the YOLO extension and used it on the Snapchat app. All four were inundated with harassing, obscene, and bullying messages including "physical threats, obscene sexual messages and propositions, and other humiliating comments." Users messaged A.C. suggesting that she kill herself, just as her brother had done. A.O. was sent a sexual message, and her friend was told she was a "whore" and "boy-obsessed." A.K. received death threats, was falsely accused of drug use, mocked for donating her hair to a cancer charity, and exhorted to "go kill [her]self," which she seriously considered. She suffered for years thereafter. Carson Bride was subjected to constant humiliating messages, many sexually explicit and highly disturbing. Despite his efforts, Carson was unable to unmask the users who were sending these messages and discover their identities. On June 23, 2020, Carson hanged himself at his home.

A.K. attempted to utilize YOLO's promised unmasking feature but received no response. Carson searched the internet diligently for ways to unmask the individuals sending him harassing messages, with no success. Carson's parents continued his efforts after his death, first using YOLO's "Contact Us" form on its Customer Support page approximately two weeks

after his death. There was no answer. Approximately three months later, his mother Kristin Bride sent another message, this time to YOLO's law enforcement email, detailing what happened to Carson and the messages he received in the days before his death. The email message bounced back as undeliverable because the email address was invalid. She sent the same to the customer service email and received an automated response promising an answer that never came. Approximately three months later, Kristin reached out to a professional friend who contacted YOLO's CEO on LinkedIn, a professional networking site, with no success. She also reached out again to YOLO's law enforcement email, with the same result as before.

Kristin Bride filed suit against YOLO and other defendants no longer part of the action. The first amended complaint alleged twelve causes of action including product liability based on design defects and failure to warn, negligence, fraudulent and negligent misrepresentation, unjust enrichment, and violations of Oregon, New York, Colorado, Pennsylvania, Minnesota, and California tort law. Plaintiffs' counsel agreed at a hearing that the state law claims were all based in "misrepresentation, intentional and negligent." Forty-eight hours after Plaintiffs filed this suit, Snap suspended YOLO's access to its application and later announced a complete ban on anonymous messaging apps in its app store.

C.

Plaintiffs' theories essentially fall into two categories: products liability and misrepresentation. Counsel admitted that the state law claims all fell

under misrepresentation, and YOLO splits them between products liability and misrepresentation.

The products liability claims allege that YOLO's app is inherently dangerous because of its anonymous nature and that it was negligent for YOLO to ignore the history of teen suicides stemming from cyberbullying on anonymous apps. Plaintiffs based their products liability claim solely on the anonymity of YOLO's app at the district court and through initial briefing at this court.[1]

Plaintiffs' misrepresentation claims are based on their allegation that YOLO alerted all new users that bullying and harassing behavior would result in the offending user being banned and unmasked, but YOLO never followed through on this threat despite A.K.'s requests and Kristin Bride's emails.

The district court granted YOLO's motion to dismiss, finding that the entire complaint sought to hold YOLO responsible for the content of messages posted on its app by users and not for any separate duty or obligation to the Plaintiffs. The court relied heavily on *Dyroff v. Ultimate Software Group, Inc.*, 934 F.3d 1093 (9th Cir. 2019), which involved a lawsuit against a completely anonymous website through which the plaintiff's deceased son purchased fentanyl-laced drugs. The district court found this matter essentially on all fours with *Dyroff* and dismissed the suit.

---

[1] In their reply brief, Plaintiffs advance a new theory that several of YOLO's features taken together created liability. YOLO moved to strike this argument because it was raised for the first time in the reply brief. We agree and will grant the motion. Our grant of this motion, however, does not affect any possible motions in the district court to amend the complaint on remand.

II.

We review de novo the district court's decision to grant YOLO's motion to dismiss under Federal Rule of Civil Procedure 12(b)(6). *Puri v. Khalsa*, 844 F.3d 1152, 1157 (9th Cir. 2017). Questions of statutory interpretation are reviewed de novo as well. *Collins v. Gee W. Seattle LLC*, 631 F.3d 1001, 1004 (9th Cir. 2011). And we take all factual allegations in the complaint as true and "construe the pleadings in the light most favorable to the nonmoving party." *Rowe v. Educ. Credit Mgmt. Corp.*, 559 F.3d 1028, 1029–30 (9th Cir. 2009) (quoting *Knievel v. ESPN*, 393 F.3d 1068, 1072 (9th Cir. 2005)).

A.

The Internet was still in its infancy when Congress passed the Communications Decency Act ("CDA") in 1996. 47 U.S.C. § 230; *Batzel v. Smith*, 333 F.3d 1018, 1026–27 (9th Cir. 2003). Even at its young age, legislators recognized its tremendous latent potential. *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1099 (9th Cir. 2009). However, because of the unprecedented reach and speed of the new forum, that potential would be significantly limited if courts imposed traditional publisher liability on internet platforms. *See Doe v. Internet Brands, Inc.*, 824 F.3d 846, 851–52 (9th Cir. 2016). Traditional publisher liability held that if a publisher took upon itself the task of moderating or editing the content that appeared within its pages, it became responsible for anything tortious written there. *Id.* at 852. A New York state court perfectly illustrated this danger when it found that an online message board became a publisher responsible for the offensive content of any messages "because it deleted some

offensive posts but not others." *Id.* In light of the sheer volume of internet traffic, this presented providers with a "grim choice": voluntarily filter some content and risk overlooking problems and thereby incurring tort liability, or take a hands-off approach and let the trolls run wild. *Id.*

To address this problem, Congress enacted § 230 of the CDA. This section allows services "to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages they didn't edit or delete." *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008) (en banc) [hereinafter *Roommates*]. Congress included a policy statement within § 230 concluding that "[i]t is the policy of the United States . . . to promote the continued development of the Internet and other interactive computer services and other interactive media." 47 U.S.C. § 230(b)(1). To that end, the law sought to encourage the development and use of technologies that would allow users to filter and control the content seen by themselves or their children. *Id.* § 230(b)(3)–(4).

The operative section of the law, § 230(c), titled "Protection for 'Good Samaritan' blocking and screening of offensive material," is divided into two working parts. *Id.* § 230(c). The first broadly states that no service provider "shall be treated as the publisher or speaker of any information provided by another information content provider," or, more colloquially, by a third-party user of the service. *Id.* § 230(c)(1). The second part protects actions taken by a service provider to moderate and restrict material it "considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or

otherwise objectionable." *Id.* § 230(c)(2). Section 230 expressly preempts any state laws with which it may conflict. *Id.* § 230(e)(3).

In short, § 230 protects apps and websites which receive content posted by third-party users (i.e., Facebook, Instagram, Snapchat, LinkedIn, etc.) from liability for any of the content posted on their services, even if they take it upon themselves to establish a moderation or filtering system, however imperfect it proves to be. This immunity persists unless the service is itself "'responsible, in whole or in part, for the creation or development of' the offending content." *Roommates*, 521 F.3d at 1162 (quoting 47 U.S.C. § 230 (f)(3)).

This robust immunity applies to "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider." *Barnes*, 570 F.3d at 1100–01 (footnote omitted). The parties agree that YOLO is an interactive computer service under § 230, and therefore satisfies the first prong. *See* 47 U.S.C. § 230(f)(2). YOLO is clearly the developer of the YOLO app, which allows users to communicate anonymously, send polls and questions, and send and receive anonymous responses.

The second *Barnes* prong considers whether the cause of action alleged in the complaint seeks to plead around the CDA's strictures and treat the defendant as a "publisher or speaker" of third-party content. *See* 47 U.S.C. § 230(c)(1). "[W]hat matters is not the name of the cause of action . . . [but] whether the cause of action inherently requires the court to treat the defendant as the 'publisher or speaker' of content

provided by another." *Barnes*, 570 F.3d at 1101–02 (listing successful cases against services that failed to qualify for § 230 immunity). The act of "publication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content." *Id.* at 1102.

It is imperative to consider that "neither [subsection 230(c)] nor any other declares a general immunity from liability deriving from third-party content." *Id.* at 1100. Indeed, that could not be true; for most applications of § 230 in our internet age involve social media companies, which nearly all provide some form of platform for users to communicate with each other. In cases such as these, "[p]ublishing activity is a but-for cause of just about everything [defendants are] involved in. [They are] internet publishing business[es]." *Internet Brands*, 824 F.3d at 853; *see also Calise v. Meta Platforms, Inc.*, 103 F.4th 732, 742 (9th Cir. 2024) ("Putting these cases together, it is not enough that a claim, including its underlying facts, stems from third-party content for § 230 immunity to apply."). The proper analysis requires a close examination of the duty underlying each cause of action to decide if it "derives from the defendant's status or conduct as a publisher or speaker." *Barnes*, 570 F.3d at 1107. Therefore, services can still be liable under traditional tort theories if those theories do not require the services to exercise some kind of publication or editorial function. *Id.* at 1102.

B.

In short, we must engage in a "careful exegesis of the statutory language" to determine if these claims attempt to treat YOLO as the "publisher or speaker"

of the allegedly tortious messages. *Id.* at 1100. This exacting analysis helps us avoid "exceed[ing] the scope of the immunity provided by Congress."[2] *Internet Brands*, 824 F.3d at 853 (quoting *Roommates*, 521 F.3d at 1164 n.15). After all, § 230 immunity is extraordinarily powerful, granting complete immunity where it applies and, in the process, preempting even the will of the people as expressed in their state legislatures. *See* 47 U.S.C. §230(e)(3) (preempting state law). Our analysis, therefore, "ask[s] whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a 'publisher or speaker.' If it does, section 230(c)(1) precludes liability." *Barnes*, 570 F.3d at 1102. But if it does not, then the suit may proceed as against the claim of immunity based on § 230(c)(1).

Our opinion in *Calise v. Meta Platforms*, published earlier this year, clarified the required duty analysis that originated in *Barnes v. Yahoo*, *Lemmon v. Snap, Inc.*, and *HomeAway.com, Inc. v. City of Santa Monica*. *Calise*, 103 F.4th at 742 ("Our cases instead require us to look to the legal 'duty.' 'Duty' is 'that which one is bound to do, and for which somebody else has a corresponding right.'" (quoting *Duty*, Black's Law Dictionary (11th ed. 2019))). We now conduct a two-step analysis. *Id.* First, we examine the "right from which the duty springs." *Id.* (quotations omitted). Does it stem from the platform's status as a publisher (in which case it is barred by § 230)? Or does it spring from some other obligation, such as a promise or contract (which,

---

[2] In light of this, we have explicitly disclaimed the use of a "but-for" test because it would vastly expand § 230 immunity beyond Congress' original intent. *See Internet Brands*, 824 F.3d at 853.

under *Barnes*, is distinct from publication and not barred by § 230)? Second, we ask what "this duty requir[es] the defendant to do." *Id.* If it requires that YOLO moderate content to fulfill its duty, then § 230 immunity attaches.[3] *See id.*; *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019).

Barnes perfectly illustrates the duty distinction reemphasized in *Calise*. In that case, Barnes's estranged boyfriend posted nude images of her on a fake profile on Yahoo's website, and she reached out to Yahoo to get them removed. *Barnes*, 570 F.3d at 1098–99. Yahoo's Director of Communications promised Barnes over the phone that she would personally facilitate the removal of the offending fake profile. *Id.* at 1099. Nothing happened and Barnes sued, alleging negligent undertaking and promissory estoppel. *Id.* Skeptical of Barnes's negligent undertaking claim, we held that it was simply a defamation claim recast as negligence and asked,

> [W]hat is the undertaking that Barnes alleges Yahoo failed to perform with due care? The removal of the indecent profiles that her former boyfriend posted on Yahoo's website. But removing content is something publishers do, and to impose liability on the

---

[3] We emphasize, however, that this does not mean immunity attaches anytime YOLO could respond to a legal duty by removing content. *See HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019). Instead, we look at what the purported legal duty *requires*— "specifically, whether the duty would necessarily require an internet company to monitor third-party content." *Id.* For immunity to attach at this second step, moderation must be more than one option in YOLO's menu of possible responses; it must be the only option.

> basis of such conduct necessarily involves treating the liable party as a publisher of the content it failed to remove.

Id. at 1103; *see* 47 U.S.C. § 230(c)(1). We determined that Barnes's negligent undertaking claim faulted Yahoo for failure to remove content, and "such conduct is publishing conduct . . . that can be boiled down to" editorial behavior. *Id.* at 1103 (emphasis and quotations omitted) (quoting *Roommates*, 521 F.3d at 1170–71). Such claims are explicitly foreclosed by § 230(c)(1).

Barnes's promissory estoppel claim, however, fared better. Because this claim "is a subset of a theory of recovery based on a breach of contract," it was not ultimately grounded in Yahoo's failure to remove content, but in their failure to honor a "private bargain[]." *Id.* at 1106 (quotations omitted). While yes, that was a promise to moderate content, the underlying obligation upon which Barnes relied was not an obligation to remove a profile, but the promise itself. *Id.* at 1107–09. As we noted, Barnes did "not seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promisor who [had] breached." *Id.* at 1107. Section 230 only "precludes liability when the duty the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a publisher or speaker." *Id.* We justified the distinction because of where the individual claims derive liability: negligent undertaking is grounded in "behavior that is identical to publishing or speaking," whereas "[p]romising is different because it is not synonymous with the performance of the action promised." *Id.* "[W]hereas one cannot undertake to do something without simultaneously doing it, one can, and often does, promise to do

something without actually doing it at the same time." *Id.* Therefore, contractual liability stood where negligence fell.

The question of whether § 230 immunity applies is not simply a matter of examining the record to see if "a claim, including its underlying facts, stems from third-party content." *Calise*, 103 F.4th at 742. Nor is there a bright-line rule allowing contract claims and prohibiting tort claims that do not require moderating content, for that would be inconsistent with those cases where we have allowed tort claims to proceed, *see Internet Brands*, 824 F.3d 846 (negligent failure to warn claim survived § 230 immunity); *Lemmon v. Snap, Inc.*, 995 F.3d 1085 (9th Cir. 2021) (authorizing a products liability claim based in negligent design), and contradict our prior position that the name of a cause of action is irrelevant to immunity, *Barnes*, 570 F.3d at 1102 ("[W]hat matters is not the name of the cause of action . . . what matters is whether the cause of action inherently requires the court to treat the defendant as the 'publisher or speaker' of content provided by another."). Instead, we must engage in a careful inquiry into the fundamental duty invoked by the plaintiff and determine if it "derives from the defendant's status or conduct as a 'publisher or speaker.'" *Id.*

C.

We now conduct that inquiry here. The parties divide the claims into two categories—misrepresentation and products liability—and we will continue that distinction in our analysis.

1.

Turning first to Plaintiffs' misrepresentation claims, we find that *Barnes* controls. YOLO's representation to its users that it would unmask and ban abusive users is sufficiently analogous to Yahoo's promise to remove an offensive profile. Plaintiffs seek to hold YOLO accountable for a promise or representation, and not for failure to take certain moderation actions. Specifically, Plaintiffs allege that YOLO represented to anyone who downloaded its app that it would not tolerate "objectionable content or abusive users" and would reveal the identities of anyone violating these terms. They further allege that all Plaintiffs relied on this statement when they elected to use YOLO's app, but that YOLO never took any action, even when directly requested to by A.K. In fact, considering YOLO's staff size compared to its user body, it is doubtful that YOLO ever intended to act on its own representation.

While it is certainly an open question whether YOLO has any defenses to enforcement of its promise, at this stage we cannot say that § 230 categorically prohibits Plaintiffs from making the argument. YOLO may argue that it did not intend to induce reliance on the promise by the Plaintiffs, or that the statements were not promises made to Plaintiffs but instead warnings to others. But we treat "the outwardly manifested intention to create an expectation on the part of another as a legally significant event. That event generates a legal duty distinct from the conduct at hand," a duty which we will enforce. *Barnes*, 570 F.3d at 1107.

The district court oversimplified the proper analysis for § 230 immunity and essentially dismissed the

claims because malicious third-party postings were involved or must be edited by YOLO. In its own words, "Plaintiffs' claims that [YOLO] . . . misrepresented their applications' safety would not be cognizable" without the harmful behavior of third-party users, and therefore immunity applies. The proper analysis is to examine closely the duty underlying each cause of action and decide if it "derives from the defendant's status or conduct as a publisher or speaker." *Id.* If it does, then § 230(c)(1) immunizes the defendant from liability on that claim.

In summary, *Barnes* is on all fours with Plaintiffs' misrepresentation claims here. YOLO repeatedly informed users that it would unmask and ban users who violated the terms of service. Yet it never did so, and may have never intended to. Plaintiffs seek to enforce that promise—made multiple times to them and upon which they relied—to unmask their tormentors. While yes, online content is involved in these facts, and content moderation is one possible solution for YOLO to fulfill its promise, the underlying duty being invoked by the Plaintiffs, according to *Calise*, is the promise itself. *See Barnes*, 570 F.3d at 1106–09. Therefore, the misrepresentation claims survive.

2.

Next, we address the product liability claims. In general, these claims assert that YOLO's app is inherently dangerous because of its anonymous nature, and that previous high-profile suicides and the history of cyberbullying should have put YOLO on notice that its product was unduly dangerous to teenagers. We hold that § 230 precludes liability on these claims.

Plaintiffs first allege product liability claims for design defect, and negligence. The defective design claim alleges that YOLO "developed, designed, manufactured, marketed, sold, and distributed to at least hundreds of thousands of minors" a product that was unreasonably dangerous because of its anonymity. They claim that the bare fact of YOLO's anonymity made it uniquely dangerous to minors and that YOLO should have known this because prior anonymous applications had a deleterious effect on minor users. The negligence claim is similar, claiming that YOLO failed to "protect users from an unreasonable risk of harm arising out of the use of their app[]." Failure to mitigate this "foreseeable risk of harm," Plaintiffs claim, makes YOLO liable.

Plaintiffs also allege products liability claims under a failure to warn theory. The alleged risks are the same as those for defective design and negligence, but the claims are centered more on YOLO's alleged failure to disclose these risks to users when they downloaded the YOLO app. Plaintiffs therefore ask for compensatory damages, pecuniary loss, and loss of society, companionship, and services to Carson Bride's parents, and punitive damages "based on [YOLO's] willful and wanton failure to warn of the known dangers" of its product.

At root, all Plaintiffs' product liability theories attempt to hold YOLO responsible for users' speech or YOLO's decision to publish it. For example, the negligent design claim faults YOLO for creating an app with an "unreasonable risk of harm." What is that harm but the harassing and bullying posts of others? Similarly, the failure to warn claim faults YOLO for not mitigating, in some way, the harmful effects of the

harassing and bullying content. This is essentially faulting YOLO for not moderating content in some way, whether through deletion, change, or suppression.

Our decision in *Lemmon v. Snap, Inc.* does not help Plaintiffs. In that case, parents of two teens killed while speeding sued the company that owns Snapchat. *Lemmon*, 995 F.3d at 1087. They alleged that the boys had been speeding because of a feature on the Snapchat app that allowed users to overlay their current speed onto photos and videos. *Id.* at 1088–89. It was widely believed that Snapchat would reward users with in-app rewards of some kind if they attained a speed over 100 mph. *Id.* at 1089. The boys operated the filter moments before their deaths. *Id.* at 1088. The parents brought negligent design claims alleging that Snapchat, despite numerous news articles, an online petition about the inherent problems with the filter, "at least three accidents," and "at least one other lawsuit," continued to offer a feature that "incentiviz[ed] young drivers to drive at dangerous speeds." *Id.* at 1089. The district court dismissed the complaint on § 230 grounds. *Id.* at 1090. On appeal, we held that the negligent design claims were not an attempt "to treat a defendant as a 'publisher or speaker' of third-party content." *Id.* at 1091. Instead, the parents sought to hold Snap liable for creating (1) Snapchat, (2) the speed filter, and (3) an incentive structure that enticed users to drive at unsafe speeds. *Id.* In clarifying that the parents' product liability claim was not "a creative attempt to plead around the CDA," we explained that claim did "not depend on what messages, if any, a Snapchat user employing the Speed Filter actually sends." *Id.* at 1094. As a result, the claim did not depend on third-party content. *Id.*

Here, Plaintiffs allege that anonymity itself creates an unreasonable risk of harm. But we refuse to endorse a theory that would classify anonymity as a per se inherently unreasonable risk to sustain a theory of product liability. First, unlike in *Lemmon*, where the dangerous activity the alleged defective design incentivized was the dangerous behavior of speeding, here, the activity encouraged is the sharing of messages between users. *See id.* Second, anonymity is not only a cornerstone of much internet speech, but it is also easily achieved. After all, verification of a user's information through government-issued ID is rare on the internet. Thus we cannot say that this feature was uniquely or unreasonably dangerous.

Similarly, *Internet Brands* provides no cover for Plaintiffs' failure to warn theory. In that case, we upheld liability against a professional networking site for models under a failure to warn theory. *Internet Brands*, 824 F.3d at 848. Plaintiff created a profile on the website Model Mayhem, owned by Internet Brands, advertising her services as a model. *Id.* Meanwhile, the site's owners were aware that a pair of men had been using the site to set up fake auditions, lure women to "auditions" in Florida, and then rape them. *Id.* at 848–49. Yet the owners did not warn plaintiff, and she fell victim to the scheme. *Id.* at 848. We reasoned that plaintiff sought to hold defendant liable under a traditional tort theory—the duty to warn—which had no bearing on Model Mayhem's decision to publish any information on its site. *Id.* at 851. After all, plaintiff had posted her own profile on the website, and did not allege that the rapists had posted anything on the website. *Id.* Therefore, § 230 was no protection.

In short, the defendant in *Internet Brands* failed to warn of a known conspiracy operating independent of the site's publishing function. *Id.* But here, there was no conspiracy to harm that could be defined with any specificity. It was merely a general possibility of harm resulting from use of the YOLO app, and which largely exists anywhere on the internet. We cannot hold YOLO responsible for the unfortunate realities of human nature.

Finally, we clarify the extent to which *Dyroff v. Ultimate Software Group* is applicable, but not dispositive, here. In that case, a grieving mother sued an anonymous website that allowed users to post whatever they wanted, anonymously, and receive anonymous replies. *Dyroff*, 934 F.3d at 1094– 95. Her son purchased drugs using the site and died because the drugs he purchased were laced with fentanyl. *Id.* at 1095. As we explained, "[s]ome of the site's functions, including user anonymity and grouping, facilitated illegal drug sales." *Id.* at 1095. The mother sued, alleging that the site had allowed users to engage in illegal activity, that the website's recommendation algorithm had promoted and enabled these communications, and that defendant failed to moderate the website's content to eliminate these problems. *Id.* We concluded that § 230(c) granted defendant immunity from these claims. *Id.* at 1096. First, we noted that § 230 "provides that website operators are immune from liability for third-party information . . . unless the website operator 'is responsible, in whole or in part, for the creation or development of [the] information.'" *Id.* (brackets in original) (quoting 47 U.S.C. § 230(c)(1), (f)(3)). We then looked at whether the claims "inherently require[] the court to treat the defendant as the 'publisher

or speaker' of content provided by another." *Id.* at 1098 (brackets in original) (quoting *Barnes*, 570 F.3d at 1102). Because the automated processes contained in the site's algorithm were not themselves content but merely "tools meant to facilitate the communication and content of others," we found the second *Barnes* prong satisfied. *Id.* Finally, the third *Barnes* prong was satisfied because the content was clearly developed by others, not the defendant. *Id.* at 1098. Unlike in *Roommates*, where the defendant played a role in developing the illegal content by requiring users to answer particular questions, the defendant in *Dyroff* merely provided a "blank text box" that users could utilize however they wanted. *Id.* at 1099.

In our view, Plaintiffs' product liability theories similarly attempt to hold YOLO liable as a publisher of third-party content, based in part on the design feature of anonymity. To be sure, our opinion in *Dyroff* did not rely on anonymity for its § 230 analysis. *See id.* at 1096–99. But our analysis of Plaintiffs' product liability claims is otherwise consistent with *Dyroff*'s reasoning: here, the communications between users were direct, rather than suggested by an algorithm, and YOLO similarly provided users with a blank text box. These facts fall within *Dyroff*'s ambit. As we have recognized, "No website could function if a duty of care was created when a website facilitates communication, in a content-neutral fashion, of its users' content." *Id.* at 1101. Though the claims asserted in *Dyroff* were different than the claims asserted here, our conclusion is consistent with *Dyroff*'s reasoning.

In summary, Plaintiffs' product liability claims attempt to hold YOLO responsible as the speaker or publisher of harassing and bullying speech. Those

product liability claims that fault YOLO for not moderating content are foreclosed, *see supra* at 18; otherwise, nothing about YOLO's app was so inherently dangerous that we can justify these claims, and unlike *Lemmon*, YOLO did not turn a blind eye to the popular belief that there existed in-app features that could only be accessible through bad behavior. *Lemmon*, 995 F.3d at 1089–90 (describing how users thought that exceeding 100 mph while using the Snapchat app would produce a reward). And to the degree that the online environment encouraged and enabled such behavior, that is not unique to YOLO. It is a problem which besets the entire internet. Thus, § 230 immunizes YOLO from liability on these claims.

D.

In holding that the Plaintiffs' misrepresentation claims may proceed, we adhere to long-established circuit precedent. We must strike a delicate balance by giving effect to the intent of Congress as expressed in the statute while not expanding the statute beyond the legislature's expressed intent in the face of quickly advancing technology. Today's decision does not expand liability for internet companies or make all violations of their own terms of service into actionable claims. To the degree that such liability exists, it already existed under *Barnes* and *Calise*, and nothing we do here extends that legal exposure to new arenas. Section 230 prohibits holding companies responsible for moderating or failing to moderate content. It does not immunize them from breaking their promises. Even if those promises regard content moderation, the promise itself is actionable separate from the moderation action, and that has been true at least since *Barnes*. In our caution to ensure § 230 is given its

fullest effect, we must resist the corollary urge to extend immunity beyond the parameters established by Congress and thereby create a free-wheeling immunity for tech companies that is not enjoyed by other players in the economy.

III.

We therefore REVERSE the district court's grant of YOLO's motion to dismiss the misrepresentation claims but AFFIRM in all other respects. YOLO's motion to strike is GRANTED.

ORDER GRANTING DEFENDANTS' JOINT MOTION TO DISMISS, U.S. DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA (JANUARY 10, 2023)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

KRISTIN BRIDE, ET AL.

v.

SNAP INC., ET AL.

CIVIL MINUTES – GENERAL

Case No.: 2:21-cv-06680-FWS-MRW

Present: Hon. Fred W. SLAUGHTER, U.S. District Judge.

PROCEEDINGS: ORDER GRANTING DEFENDANTS' JOINT MOTION TO DISMISS [118][127]

Before the court are Defendants Yolo Technologies, Inc. ("Yolo") and LightSpace Inc.'s ("LightSpace") (collectively, "Defendants") Motions to Dismiss Plaintiffs the Estate of Carson Bride by and through his appointed administrator, Kristin Bride, A.C., A.O.,

A.K.,[1] and the Tyler Clementi Foundation's ("Plaintiffs") First Amended Complaint ("FAC"). (Dkts. 118, 127.) The matter is fully briefed.[2] (Dkts. 135, 138-39.) Based on the state of the record, as applied to the applicable law, the court **GRANTS** the Motion and **DISMISSES WITH PREJUDICE** the **FAC**.

I. Relevant Background

The FAC alleges[3] that Yolo and LightSpace designed, developed, and operate the YOLO and LMK applications, respectively, which have "Teen" content ratings on the Google Play store, and permit teenaged and minor users to share anonymous messages. (Dkt. 113 ¶¶ 60, 74-76.) LMK is an "anonymous Question and Answer and polling app" that allows its users to "create and customize[] stickers and backgrounds while sharing polls with their friends on Snapchat." (*Id.* ¶¶ 28, 73.) Similarly, YOLO "is an app designed to allow its users to send messages to each other anonymously" who can "chat, exchange questions and answers, and send polling requests to one another on

---

[1] A.C., A.O., and A.K., are represented by and through their legal guardians, Jane Does 2, 3, and 1, respectively.

[2] The court, in its discretion, GRANTS Plaintiffs' Motion to Exceed the Page Limit in Opposition to Defendant's Motion to Dismiss by five (5) pages. (Dkt. 137.) While Yolo opposes, (Dkt. 140), the court finds any resulting prejudice minimal and that it is in the interest of judicial economy to permit the brief as filed. Future requests of this nature must be set for hearing in advance of the motion to which they relate.

[3] For the purposes of the Motions to Dismiss, the court accepts all allegations of material fact as true and construes the pleadings in the light most favorable to Plaintiffs. *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

a completely anonymous basis." (*Id.* ¶ 26.) Senders of messages on YOLO and LMK remain anonymous. (*Id.* ¶¶ 3, 56, 73.) Plaintiffs allege studies show the "depersonalized" context of anonymous apps increases the risk of "aberrant" behavior like bullying and harassment. (*Id.* ¶¶ 35-37.)

Plaintiffs allege they received harassing messages in response to their benign posts on Defendants' applications and did not receive comparable messages on other platforms in which user identities were revealed. (*Id.* ¶¶ 97-99, 102-104.) Plaintiffs allege that YOLO had pop-up notifications that stated individuals' identities would be revealed if they harassed other users and LightSpace similarly stated it would take reports of bullying it received seriously and potentially send those reports to law enforcement. (*Id.* ¶¶ 65, 71, 81, 105-118.) Plaintiffs reference several specific explicit messages they received on these platforms and also aver more generally that they received harassing messages on both applications. (*Id.* ¶¶ 90-103, 128-131, 136-140, 145-147.) Plaintiffs allege that YOLO in particular did not respond to reports of harassment and that a decedent of one of the Plaintiffs unsuccessfully attempted to search online for ways to "reveal" the identities of individuals who had previously sent him harassing messages on YOLO the night before his death. (*See id.* ¶¶ 71, 94.)

In this lawsuit, Plaintiffs bring state law causes of action against Defendants for: (1) strict product liability based on a design defect; (2) strict product liability based on a failure to warn; (3) negligence; (4) fraudulent misrepresentation; (5) negligent misrepresentation; (6) unjust enrichment; (7) violation of the Oregon Unlawful Trade Practices Act; (7) violation of

the New York General Business Law § 349; (8) violation of the New York General Business Law § 350; (9) violation of the Colorado Consumer Protection Act; (10) violation of the Pennsylvania Unfair Trade Practices Law; (11) violation of the Minnesota False Statement in Advertising Act; and (12) violation of California Business and Professions Code §§ 17200 & 17500. (*See id.* ¶¶ 20-30, 178-322.) Plaintiffs seek to bring a class action. (*See id.* ¶¶ 159-177.)

Plaintiffs initially filed the Complaint in this action on May 10, 2021, against Defendants and former Defendant Snap, Inc., in the Northern District of California. (Dkt. 1.) The case was transferred to the Central District of California on August 18, 2021. (Dkts. 49-50, 53.) The three Defendants initially filed Motions to Dismiss and Stay Discovery in September 2021, (*see* Dkts. 71-77, 79); after numerous stipulations to extend the hearing on those motions pending settlement discussions, (*see* Dkts. 82, 86, 88, 90, 94, 96, 98, 102, 105), the parties stipulated to Snap, Inc.'s dismissal with prejudice from this action on June 17, 2022, (Dkt. 111). Plaintiff filed the First Amended Complaint on June 27, 2022. (Dkt. 113.) After several more stipulations to extend the deadlines in this case, (Dkts. 112, 116, 121, 123), the court entered an order on September 29, 2022, granting Defendants' motion to stay discovery pending resolution of potentially dispositive motions to dismiss, (Dkt. 126). LightSpace initially moved to dismiss the FAC on August 18, 2022, (Dkt. 118), and Yolo similarly moved on October 6, 2022, (Dkt. 127). The court heard oral argument on these matters on January 5, 2023. (Dkt. 141.)

II. Legal Standard

A. Motion to Dismiss Pursuant to Rule 12(b)(6)

Rule 12(b)(6) permits a defendant to move to dismiss a complaint for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). "[C]ourts must consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 322 (2007). To withstand a motion to dismiss brought under Rule 12(b)(6), a complaint must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). While "a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations," a plaintiff must provide "more than labels and conclusions" and "a formulaic recitation of the elements of a cause of action" such that the factual allegations "raise a right to relief above the speculative level." *Id.* at 555 (citations and internal quotation marks omitted); *see also Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009) (reiterating that "recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice"). "A Rule 12(b)(6) dismissal 'can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory.'" *Godecke v. Kinetic Concepts, Inc.*, 937 F.3d 1201, 1208 (9th Cir. 2019) (quoting *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990)).

"Establishing the plausibility of a complaint's allegations is a two-step process that is 'context-specific' and 'requires the reviewing court to draw on its judicial experience and common sense.'" *Eclectic Props. E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 995-96 (9th Cir. 2014) (quoting *Iqbal*, 556 U.S. at 679). "First, to be entitled to the presumption of truth, allegations in a complaint . . . must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Id.* at 996 (quoting *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011)). "Second, the factual allegations that are taken as true must plausibly suggest an entitlement to relief, such that it is not unfair to require the opposing party to be subjected to the expense of discovery and continued litigation." *Id.* (quoting *Starr*, 652 F.3d at 1216); *see also Iqbal*, 556 U.S. at 681.

Plausibility "is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. 544, 556 (2007)). On one hand, "[g]enerally, when a plaintiff alleges facts consistent with both the plaintiff's and the defendant's explanation, and both explanations are plausible, the plaintiff survives a motion to dismiss under Rule 12(b)(6)." *In re Dynamic Random Access Memory (DRAM) Indirect Purchaser Antitrust Litig.*, 28 F.4th 42, 47 (9th Cir. 2022) (citing *Starr*, 652 F.3d at 1216). But, on the other, "'[w]here a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief.'" *Eclectic Props. E., LLC*, 751 F.3d at 996 (quoting *Iqbal*, 556 at U.S.

678). Ultimately, a claim is facially plausible where "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *See Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 at 556); *accord Wilson v. Hewlett-Packard Co.*, 668 F.3d 1136, 1140 (9th Cir. 2012).

In *Sprewell v. Golden State Warriors*, the Ninth Circuit described legal standards for motions to dismiss made pursuant to Rule 12(b)(6):

> Review is limited to the contents of the complaint. *See Enesco Corp. v. Price/Costco, Inc.*, 146 F.3d 1083, 1085 (9th Cir. 1998). All allegations of material fact are taken as true and construed in the light most favorable to the nonmoving party. *See id.* The court need not, however, accept as true allegations that contradict matters properly subject to judicial notice or by exhibit. *See Mullis v. United States Bankr. Ct.*, 828 F.2d 1385, 1388 (9th Cir.1987). Nor is the court required to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences. *See Clegg v. Cult Awareness Network*, 18 F.3d 752, 754-55 (9th Cir. 1994).

266 F.3d 979, 988 (9th Cir. 2001).

III. Discussion

A. Section 230 of the Communications Decency Act

Defendants first argue that they are immune from suit under Section 230 of the Communications

Decency Act of 1996 ("CDA"), 47 U.S.C. § 230. Section 230 of the CDA "protects certain internet-based actors from certain kinds of lawsuits." *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1099 (9th Cir. 2009). The statute provides, in relevant part, that "[n]o 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." 47 U.S.C. § 230(c)(1). Additionally, it states that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." *Id.* § 230(e)(3). "The majority of federal circuits have interpreted the CDA to establish broad federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service." *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir. 2007) (citations and internal quotation marks omitted).

CDA immunity under Section 230(c)(1) "applies only if the interactive computer service provider is not also an 'information content provider,' which is defined as someone who is 'responsible, in whole or in part, for the creation or development of' the offending content." *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1162 (9th Cir. 2008) (en banc) (quoting 47 U.S.C. § 230(f)(3)). The "prototypical service qualifying for [CDA] immunity is an online messaging board (or bulletin board) on which Internet subscribers post comments and respond to comments posted by others." *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1266 (9th Cir. 2016) (quoting *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1195 (10th Cir. 2009)).

Under the Ninth Circuit's three-prong test, "[i]mmunity from liability exists for '(1) a provider or

user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider.'" *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1097 (9th Cir. 2019) (quoting *Barnes*, 570 F.3d at 1100-01). "When a plaintiff cannot allege enough facts to overcome Section 230 immunity, a plaintiff's claims should be dismissed." *Id.* (citation omitted).

In considering the first prong of the *Barnes* test, courts "interpret the term 'interactive computer service' expansively." *Id.* (citation omitted). Here, Plaintiffs do not meaningfully challenge Defendants' status as providers of "interactive computer service[s]" within the meaning of Section 230. (*See* Dkt. 135 at 5-30.) Under the statute, "[t]he 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." 47 U.S.C. § 230(f)(2). Courts have noted providers of interactive computer services include entities that create, own, and operate applications that enable users to share messages over its internet-based servers, like Defendants. *See, e.g.*, *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1091 (9th Cir. 2021) (holding creator, owner, and operator of application that "permits its users to share photos and videos through [its] servers and the internet" necessarily "enables computer access by multiple users to a computer server," and thus qualifies as a "provider of an interactive computer service") (citations and internal quotation marks

omitted). Accordingly, the court finds the first prong of the *Barnes* test is met.

Under the second prong, "what matters is whether the claims 'inherently require[] the court to treat the defendant as the "publisher or speaker" of content provided by another.'" *Dyroff*, 934 F.3d at 1098 (alteration in original) (quoting *Barnes*, 570 F.3d at 1102). Plaintiffs argue their claims do not treat Defendants as publishers or speakers because their claims allege Defendants' products could be made safer without altering third-party content and that the designs of Defendants' applications encourage the alleged harmful conduct. (Dkt. 135 at 6-12.) Further, Plaintiffs argue the anonymity of Defendants' users "itself creates harm that makes any content seem harmful." (Dkt. 135 at 11-12.) Defendants contend that, regardless of how Plaintiffs' claims are styled, Plaintiffs' legal theories seek to hold Defendants liable for publishing the content of third parties. (Dkts. 118 at 9-10; 127 at 14-15.)

Ultimately, although Plaintiffs frame user anonymity as a defective design feature of Defendants' applications, Plaintiffs fundamentally seek to hold Defendants liable based on content published by anonymous third parties on their applications. Accordingly, the court finds Plaintiff's theories of liability treat Defendants as a "publisher" within the meaning of Section 230. *See Dyroff*, 934 F.3d at 1098 (acknowledging defendant implemented "features and functions" to "analyze" and "recommend" user grounds but holding plaintiffs "cannot plead around Section 230 immunity by framing these website features as content" because plaintiffs' claims sought to treat defendant as a "publisher" of third-party information); *id.* at 1095

(noting that "[s]ome of [defendant's] [web]site's functions, including user anonymity and grouping, facilitated illegal drug sales"); *Kimzey*, 836 F.3d 1266 (holding district court properly dismissed complaint that sought to "circumvent the CDA's protections" by "plead[ing] around the CDA to advance the same basic argument that the statute plainly bars: that [defendant] published user-generated speech that was harmful to [plaintiff]") (citation omitted); *Gonzalez v. Google LLC*, 2 F.4th 871, 891 (9th Cir. 2021), *cert. granted*, 143 S. Ct. 80 (2022) ("This element is satisfied when 'the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a "publisher or speaker."'") (quoting *Barnes*, 570 F.3d at 1102); *see also Force v. Facebook, Inc.*, 934 F.3d 53, 65 (2d Cir. 2019) (noting "[t]he courts' generally broad construction of Section 230(c)(1) in favor of immunity has resulted in a capacious conception of what it means to treat a website operator as the publisher of information provided by a third party") (cleaned up). While Plaintiffs urge that preventing users from posting anonymously is unrelated to the content users of Defendants' applications generate, these "decisions about the structure and operation of a website are content-based decisions" under Section 230. *See Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116, 1124 (N.D. Cal. 2016) (noting courts have held such content-based decisions include "the option to anonymize email addresses, [and the] acceptance of anonymous payments") (citing *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 20 (1st Cir. 2016)); *see also Lewis v. Google LLC*, 461 F. Supp. 3d 938, 954 (N.D. Cal. 2020).

The court similarly finds that *Dyroff* is not materially distinguishable on the basis that the users of the application at issue in *Dryoff* remained pseudonymous while posting users of Defendants' applications remain anonymous. The Ninth Circuit in *Dyroff* drew no such distinction. Rather, the Circuit stated that "[t]oday, online privacy is a ubiquitous public concern for both users and technology companies." 934 F.3d at 1100. The Ninth Circuit in *Dryoff* spoke in terms of "anonymity," not pseudonymity. *See id.* at 1095, 1100. Even if it had not, the court does not find it plausible to distinguish from *Dyroff* given the Ninth Circuit ultimately concluded that the defendant was "entitled to immunity under the plain terms of Section 230 and our case law as a publisher of third-party content" because the plaintiff could not "and [did] not plead that [the defendant] required users to post specific content, made suggestions regarding the content of potential user posts, or contributed to making unlawful or objectionable user posts." *Id.* at 1099. The court finds this ultimate conclusion applies to this case with equal force.

Plaintiffs principally seek to combat the application of Section 230 immunity by bringing this case within the ambit of *Lemmon*, in which the plaintiffs brought claims against Snap, Inc., a former Defendant in this case and creator of an application similar to Defendants'. In *Lemmon*, the plaintiffs alleged Snapchat's "Speed Filter," an "interactive system" that "encouraged its users to pursue certain unknown achievements and rewards" and "worked in tandem to entice young Snapchat users to drive at speeds exceeding 100 MPH," had nothing to do with "its editing, monitoring, or removing of the content that its users generate

through Snapchat." 995 F.3d at 1091-92. Finding the case presented "a clear example of a claim that simply does not rest on third-party content," *id.* at 1093, the Ninth Circuit held that "the duty [Snap] allegedly violated 'spr[a]ng[] from' its distinct capacity as a product designer,'" *id.* at 1092. The Ninth Circuit in *Lemmon* also reasoned 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." *Id.* (citing *Internet Brands*, 824 F.3d at 851).

Though Plaintiffs seek to characterize anonymity as a feature or design independent of the content posted on Defendants' applications, the theories underlying Plaintiffs' claims essentially reduce to holding Defendants liable for publishing content created by third parties that is allegedly harmful because the speakers are anonymous. Imposing such a duty would "necessarily require [Defendants] to monitor third-party content," *cf. HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019), e.g., in the form of requiring Defendants to ensure that each user's post on their applications is traceable to a specifically identifiable person. Accordingly, the court finds *Lemmon* is distinguishable, and the second prong of Section 230 immunity is satisfied.

Under the third prong, "§ 230(c)(1) cuts off liability only when a plaintiff's claim faults the defendant for information provided by third parties" but permits liability against internet companies when "they create or develop their own internet content" or are "responsible in part, for the creation or the development of the offending content on the internet." *Lemmon*, 995

F.3d at 1093 (cleaned up). Here, Plaintiffs argue their claims do not treat Defendants as publishers of information, but rather seek to impose liability on the basis that their applications could have been designed more safely without altering third-party content; namely, by removing complete anonymity. (Dkt. 135 at 5-10.) Plaintiffs also argue that Defendants contributed to the behavior that harmed Plaintiffs by designing applications in which posting users remain anonymous, thereby promoting bullying on their platforms. (*Id.* at 10-12.) Defendants argue that their users, not Defendants, are the persons responsible for the creation or development of the harmful content at issue. (Dkts. 118 at 8-9; 127 at 14.)

The thrust of Plaintiffs' allegations concern posts by users of Defendants' applications. Accordingly, Defendants are not "information content provider[s] because [they] did not create or develop information" but rather "published information created or developed by third parties." *Dyroff*, 934 F.3d at 1098. Defendants did not create or develop the harassing and explicit messages that led to the harm suffered by Plaintiffs; the sending users did. *See id.* While Plaintiffs assert their false advertising claims differ from their other claims in this respect, (*see* Dkt. 135 at 14-15), those claims are still predicated on content developed by those third parties. Had those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable. Accordingly, the nature of Plaintiffs' legal claim does not alter the court's conclusion, whether based on negligence or false advertising. *See Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1177 (9th Cir.

2009) (noting the Ninth Circuit has held that "CDA § 230 provide[s] immunity from state unfair competition and false advertising actions") (citing *CCBill*, 488 F.3d at 1108, 1118-19)).

In sum, "[t]he accusation here is fundamentally that [Defendants] should have monitored and curbed third-party content." *See Jackson v. Airbnb, Inc.*, 2022 WL 16753197, at *2 (C.D. Cal. Nov. 4, 2022) (finding Section 230 immunized defendant notwithstanding *Lemmon* where plaintiffs' claims were "predicated on holding [defendant] liable for third party content posted on its platform"); *cf. In re Apple Inc. App Store Simulated Casino-Style Games Litig.*, 2022 WL 4009918, at *4-18 (N.D. Cal. Sept. 2, 2022) (summarizing historical development of Ninth Circuit case law regarding Section 230 and distinguishing between "mere message boards" and "creators of content themselves"). Because these claims fall squarely within Section 230's broad grant of immunity, the court finds Section 230(c)'s immunity provision applies to Defendants.

B. Applying Section 230 to Plaintiffs' Claims

As stated above, the FAC brings twelve causes of action under state law against Defendants; namely: (1) strict product liability based on a design defect; (2) strict product liability based on a failure to warn; (3) negligence; (4) fraudulent misrepresentation; (5) negligent misrepresentation; (6) unjust enrichment; (7) violation of the Oregon Unlawful Trade Practices Act; (7) violation of the New York General Business Law § 349; (8) violation of the New York General Business Law § 350; (9) violation of the Colorado Consumer Protection Act; (10) violation of the Pennsylvania

Unfair Trade Practices Law; (11) violation of the Minnesota False Statement in Advertising Act; and (12) violation of California Business and Professions Code §§ 17200 & 17500. For the reasons set forth below, the court finds that each of these causes of action is predicated on the theory that Defendants violated various state laws by failing to adequately regulate end-users' abusive messaging, and is therefore barred by Section 230.

Plaintiffs argue CDA immunity does not attach to Plaintiffs' failure to warn claims under *Doe v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016). (Dkt. 135 at 12-13.) Defendants argue *Internet Brands* is distinguishable, and that the CDA bars Plaintiffs' failure to warn claims regardless on the basis that Plaintiffs seek to hold Defendants liable as a publisher of third-party content. (Dkts. 118 at 10-14; 127 at 19-20.)

The Ninth Circuit in *Internet Brands* noted that the plaintiff sought to hold the defendant "liable for failing to warn her about information it obtained from an outside source about how third parties targeted and lured victims through [the website on which the defendant hosted the plaintiff's user profile]," and thus reasoned that "[t]he duty to warn allegedly imposed by California law would not require Internet Brands to remove any user content or otherwise affect how it publishes or monitors such content." 824 F.3d at 851. The Ninth Circuit continued that the "alleged tort based on a duty that would require such a self-produced warning falls outside of section 230(c)(1)" because the "plaintiff's negligent failure to warn claim [did] not seek to hold Internet Brands liable as the publisher or speaker of any information provided by another information content provider." *Id.* (citation

and internal quotation marks omitted). As discussed above, the court finds that Plaintiffs' theory would require the editing of third-party content, thus treating Defendants as a publisher of content. Accordingly, *Internet Brands* is inapposite on this issue.[4] *See Roommates*, 521 F.3d at 1170-71 ("[A]ny activity that can be boiled down to deciding whether to exclude material that third parties seek to post online is perforce immune under section 230."); *Dyroff*, 934 F.3d at 1100 (holding the "allegation that user anonymity equals promoting drug transactions [was] not plausible" in view of defendant's "anonymity features along with its public statements expressing concern for internet privacy and detailing the burden of law enforcement information requests" and affirming district court's "dismiss[al] [of] all claims related to this supposed theory of liability" under Section 230).

With respect to Plaintiffs' remaining claims based on negligence and various state law statutes prohibiting false advertising and misrepresentations,[5]

---

[4] Additionally, the *Internet Brands* court "express[ed] no opinion on the viability of the failure to warn allegations on the merits." 824 F.3d at 854. Later Ninth Circuit precedent suggests Defendants—whose applications' anonymous posting feature is not plausibly alleged to relate to content created or selectively promoted by Defendants—may not owe such a duty under California law, even if those claims are not barred by the CDA. *See Dyroff*, 934 F.3d at 1101 ("No website could function if a duty of care was created when a website facilitates communication, in a content-neutral fashion, of its users' content.") (citing *Klayman v. Zuckerberg*, 753 F.3d 1354, 1359-60 (D.C. Cir. 2014)).

[5] As discussed at oral argument, it is materially undisputed in substance, for the purposes of Section 230 immunity, that Plaintiffs' remaining state law claims are predicated on Plaintiffs' allegations that Defendants committed false advertising or actionable

Plaintiffs argue Section 230 immunity does not protect Defendants from their own alleged misrepresentations and false statements on which Plaintiffs' various remaining claims are based. (Dkt. 135 at 14-15.) Defendants argue that, because Plaintiffs' claims are directed at Defendants' content moderation policies, the remainder of Plaintiffs' claims are barred under the CDA. (Dkts. 118 at 15-18; 127 at 20-22.) The court agrees with Defendants and finds Plaintiffs' argument unpersuasive for the same reason as Plaintiffs' failure to warn claims: because they are all predicated on allegations concerning activity immunized by Section 230. *See Roommates*, 521 F.3d at 1170-71; *Dyroff*, 934 F.3d at 1100; *Zango*, 568 F.3d at 1177 (false advertising); *Barnes*, 570 F.3d at 1102-03 (holding negligence claim under state law that "derive[d] from [defendant's] role as a publisher" was subject to CDA immunity); *Doe through Next Friend Roe v. Snap, Inc.*, 2022 WL 2528615, at *14 (S.D. Tex. July 7, 2022) (finding state law claim based on negligence was barred by Section 230 where it was "couched as a complaint about [defendant's] design and operation rather than its role as a publisher of third-party content," because defendant's "alleged lack of safety features [was] only relevant to [plaintiff's] injuries to the extent that such features would have averted wrongful communication via [defendant's] platforms by third parties") (cleaned up).[6]

---

misrepresentations, or are otherwise coextensive with Plaintiffs' negligence or product liability claims.

[6] To the extent the Fourth Circuit's decision in *Henderson v. The Source of Public Data*, 53 F.4th 110, 122 (4th Cir. 2022), in which the Fourth Circuit Court of Appeal reinterpreted its prior conception of "publication" under § 230(c)(1) in *Zeran v. America*

Because Section 230 immunizes Defendants from Plaintiffs' claims in their entirety, the FAC is subject to dismissal.[7] "While it is black-letter law that a district court must give plaintiffs at least one chance to amend a deficient complaint, that presumption can be overcome where there has been a clear showing that amendment would be futile." *Barke v. Banks*, 25 F.4th 714, 721 (9th Cir. 2022) (cleaned up). Stated differently, although Federal Rule of Civil Procedure 15(a)(2) provides that leave to amend should be "freely" given, "that liberality does not apply when amendment would be futile." *Ebner v. Fresh, Inc.*, 838 F.3d 958, 968 (9th Cir. 2016); *see also AmerisourceBergen Corp. v. Dialysist W., Inc.*, 465 F.3d 946, 951 (9th Cir. 2006) ("[A] district court need not grant leave to amend where the amendment: (1) prejudices the opposing party; (2) is sought in bad faith; (3) produces an undue delay in litigation; or (4) is futile.") (citations omitted). "[C]ourts have treated § 230(c) immunity as quite robust," *see, e.g.*, *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123 (9th Cir. 2003), and the doctrine bars any claims brought against a covered interactive computer service provider that "inherently require[] the court to treat the defendant as the 'publisher or speaker' of content provided by another," *Dyroff*, 934 F.3d at 1098 (alteration in original) (quoting *Barnes*, 570 F.3d at 1102). Because the court finds the core

---

Online, Inc., 129 F.3d 327 (4th Cir. 1997)), is implicated here, the court finds it unpersuasive in light of broader view adopted by the Ninth Circuit, *see, e.g.*, *Roommates*, 521 F.3d at 1170-71; *see also Monsarrat v. Newman* 28 F.4th 314, 320 (1st Cir. 2022).

[7] In light of this finding that Defendants are immunized against Plaintiffs' claims under Section 230 of the CDA, the court does not reach the remainder of the parties' arguments.

theory underlying Plaintiffs' claims seeks to treat Defendants as a "publisher or speaker" of the posts of third parties utilizing their applications, the court finds amendment to be futile. *See Sikhs for Just., Inc. v. Facebook, Inc.*, 697 F. App'x 526 (9th Cir. 2017) (affirming district court's dismissal with prejudice because granting plaintiff "leave to amend its complaint would be futile" where plaintiff's claim was "barred by the CDA" under Section 230).

Ultimately, based on the state of the record, as applied to the applicable law, the court concludes that Defendants are immunized under Section 230 of the CDA and that permitting further amendment would be futile. Accordingly, the court **DISMISSES WITH PREJUDICE** the FAC.

IV. Disposition

For the reasons set forth above, the court **GRANTS** Defendants' Motions to Dismiss and **DISMISSES WITH PREJUDICE** the FAC.

IT IS SO ORDERED.

ORDER DENYING PETITION FOR REHEARING, U.S COURT OF APPEALS FOR THE NINTH CIRCUIT (SEPTEMBER 6, 2024)

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

THE ESTATE OF CARSON BRIDE, by and through his appointed administrator KRISTIN BRIDE; ET AL.,

Plaintiffs-Appellants,

v.

YOLO TECHNOLOGIES, INC.,

Defendant-Appellee.

No. 23-55134

D.C. No. 2:21-cv-06680-FWS-MRW Central District of California, Los Angeles

Before: SILER,* BEA, and IKUTA, Circuit Judges.

* The Honorable Eugene E. Siler, United States Circuit Judge for the U.S. Court of Appeals for the Sixth Circuit, sitting by designation.

ORDER

Judges Siler, Bea, and Ikuta voted to deny appellee's petition for panel rehearing.

The petition for rehearing, Dkt. No. 67, is DENIED.

STATUTORY PROVISION INVOLVED

42 U.S.C. §230. Protection for private blocking and screening of offensive material

(a) Findings

The Congress finds the following:

(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

(2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

(b) Policy

It is the policy of the United States-

(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

(3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;

(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for "Good Samaritan" blocking and screening of offensive material

(1) 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.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of-

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).1

(d) Obligations of interactive computer service

A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

(e) Effect on other laws

(1) No effect on criminal law

Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.

(2) No effect on intellectual property law

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(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.

(4) No effect on communications privacy law

Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

(f) Definitions

As used in this section:

(1) Internet

The term "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) Interactive computer service

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.

(3) Information content provider

The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

(4) Access software provider

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.

BRIEF FOR PLAINTIFFS-APPELLANTS
(AUGUST 11, 2023)

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

THE ESTATE OF CARSON BRIDE, by and through his appointed administrator KRISTIN BRIDE; A. K., by and through her legal guardian Jane Doe 1; A. C., by and through her legal guardian Jane Doe 2; A. O., by and through her legal guardian Jane Does 3; TYLER CLEMENTI FOUNDATION, on behalf of themselves and all others similarly situated,

Plaintiffs-Appellants,

v.

YOLO TECHNOLOGIES, INC.; LIGHTSPACE, INC.,

Defendants-Appellees.

23-55134

BRIEF FOR PLAINTIFFS-APPELLANTS

Juyoun Han
Eric M. Baum
Andrew Clark
Jonathan Axel
EISENBERG & BAUM, LLP
24 Union Square East, Penthouse

New York, New York 10003
(212) 353-8700

Attorneys for Plaintiffs-Appellants

{ Internal Tables of Contents, Authorities Omitted }

INTRODUCTION

"The medium is the message" is a phrase to describe how the form of a communication constructs the environment, behavior, and content of its message.[1] Marshall McLuhan writes that the medium is like a lightbulb: while light does not have any content in and of itself, it creates and develops cultural and societal content that would not otherwise have existed.[2] Acknowledging that the design of a medium has a generative effect on the resulting content becomes all the more relevant when considering the designs and features of social media platforms as communication media.

The instant case presents a tragic scenario of a 16-year-old child, Carson, who was relentlessly harassed on YOLO, a social media product with one main feature: complete anonymity of its users. Marketed to minors, the social media platform was designed to allow users to make and receive comments by others with no identifying information, such as an account ID, nickname, phone number, or tracking information.

---

[1] MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSION OF MAN, https://web.mit.edu/allanmc/www/mcluhan.mediummessage.pdf (1964).

[2] *Id.*

The anonymity-focused design of YOLO's app, offered to teenagers for free, developed a distinct culture of pervasive bullying on the platform. As Carson noted in his text conversation to his friend, the harassing comments were almost exclusively sent through YOLO, and not on other apps. YOLO's anonymity feature follows a long lineage of similarly designed products, each of which foster drama, hate, and bullying, with sometimes fatal consequences to users. The Complaint outlined these anonymous applications and the teen user-victims throughout the years who took their own lives as a result.

YOLO had another distinguishable dangerous trait: a one-sided anonymity that masks the identity of the sender of the message, but not the receiver. YOLO was designed as an add-on to Snapchat, the popular social media app for teens and children. YOLO enables users to comment on Snapchat posts without any identifying information. The receivers of YOLO messages have no control over the anonymity of the message sender, unless the anonymous sender "swipes up" and reveal their user information voluntarily. As a one-sided invisibility cloak, this YOLO feature protects users who wish to withhold their identity while keeping the message recipient in the dark – a perfect tool for cyberbullying. And the only way the receiver can respond to the anonymous bully was to make a public, non-anonymous post on their Snapchat story. Such one-sided anonymity generated the humiliation and targeted bullying that did not exist on other kinds of anonymous bulletin boards on the internet.

Adding to the recipe for chaos, YOLO then lied to young consumers that it had a safety switch—an

identity reveal—which turned out to be completely ineffective. In a conspicuous statement contained in a bold pop-up message to its users, YOLO represented that users who engage in harassment and bullying would be removed and their identities will be revealed. This safety switch was proven defective, as alleged in the Amended Complaint. Customer reviews repeatedly noted that YOLO did nothing to stop bullying, even when anonymous YOLO users encouraged children to kill themselves. Plaintiffs-Appellants experienced the same – there was no stop to the vicious comments that came through YOLO because there was no way to identify the sender(s). Carson's last moments of life were spent trying to uncover the identities of his tormentors. After Carson's death, his parents tried to contact YOLO for information about the harassment through YOLO's contact forms, emails, and even professional contacts, but received not a single response. Other Plaintiffs-Appellants were also unable to utilize YOLO's stated and advertised safety switch to reveal their harassers' identities.

As vividly demonstrated here, YOLO's anonymity feature was not an editorial function – it was the core design of the product. The product YOLO plugged into teens' phones was a "medium" of anonymity, and that medium was the message. YOLO created a virtual invisibility cloak with a falsely advertised safety switch that did not work, and reaped millions of downloads of its app—countless of those downloads were by vulnerable young users who suffered harm. And now, YOLO seeks to escape liability under a law, the Communications Decency Act, that was designed to disincentivize the exact kind of conduct seen here.

JURISDICTIONAL STATEMENT

This Court has jurisdiction under 28 U.S.C. § 1291 as an appeal from a final decision of the District Court dismissing all claims with prejudice dated January 10, 2023. ER-3. Plaintiffs timely appealed on February 9, 2023. EC-106; Fed. R. App. P. 4(a)(1)(A).

FACTUAL BACKGROUND

FOLO App – One-Sided, Anonymous Messaging App with a Defective Safety Tool

"YOLO" is an acronym for the phrase "You Only Live Once," and name of the mobile phone application ("app") developed and operated by the Defendant-Appellee, Yolo Technologies Inc. (hereinafter, YOLO). *See* ER-18 (Amended Complaint ("AC") ¶ 1). Within a week of YOLO's launch in 2019, it became the top downloaded app in America and a "teen hit," and within months the app had 10 million active users. ER-19 (AC ¶ 4).

YOLO was marketed for "teens" in app stores, inviting minors to integrate an anonymous messaging tool to the popular Snapchat platform. *See* ER-40, 46-47 (AC ¶¶ 60, 74-76). YOLO was intentionally designed with one defining feature: enabling users hide their identities when commenting on a Snapchat post (a popular social media platform whose developer, Snap, Inc., was dismissed from this case through a settlement). By using YOLO's product: (1) Snapchat users can create and publish a story (called "posting") on their account (non-anonymous) and include a question for friends or audience to answer using YOLO's anonymity tool (*see* ER-52 (AC ¶¶ 98 & 99)); (2) when another Snapchat user comments on a post, the commenter's

username is sent to the Snapchat user anonymously (*see* ER-39, 46 (*see* AC ¶¶ 56 & 73)); and (3) the anonymous commenter can voluntarily reveal themselves by "swiping up," but the receiver of the anonymous message cannot require the anonymous commenter to do so. ER-27-28, 39, 51 (*see* AC ¶¶ 26, 56 & 96). As a one-sided invisibility cloak, this YOLO feature protects users who wish to withhold their identity while keeping the message recipient in the dark – a perfect tool for cyberbullying.

It was well-known that bullying and harassment would manifest from anonymous messaging apps because this long lineage of anonymous apps that YOLO followed were already associated with teen suicides. ER-33-36 (AC ¶¶ 40-48). As Carson noted in his text conversation to his friend, the harassing comments would particularly come through YOLO, not on other apps. *See* ER-52 (AC ¶ 97).

YOLO was well-aware of this, but it made bold promises for safety on its app to users, which turned out to be a lie. When a user first opens YOLO after downloading it from the Apple or Google app stores, a pop-up notice fills the screen and tells each prospective user: "YOLO has no tolerance for objectionable content or abusive users. You'll be banned for any inappropriate usage." The Complaint alleges that Carson and all Plaintiffs-Appellants saw and relied upon this statement to their detriment. *See* ER-56, 58 (AC ¶¶ 123, 134). However, YOLO did not have any mechanism in place for investigating or responding to reports made by its users or their guardians. S*ee* ER-39, 44 (AC ¶ 57 & 70). In fact, according to YOLO's own sworn declaration in this case, fewer than 10 employees were accountable for YOLO's 10 million daily active users

as of 2021. *See* ER-39-40 (AC ¶ 58). YOLO knew that it could not possibly provide meaningful safeguards to so many active users. According to Customer Reviews, YOLO repeatedly ignored reports of dangerous levels of harassing and bullying behavior on YOLO. *See* ER-44 (AC ¶¶ 70-71) (quoting YOLO customer review: "(d) "My daughter has been getting bullied on this app and we report/block, and this bully keeps on going and it's about suicide! . . . If someone truly reports someone this nasty on the app, it should be dealt with instantly! (e) . . . At a time when suicide is the number 1 killer of teens in America, we definitely don't need apps like this where bullied haters can hide behind a screen (g) . . . it's teaching our youth that it's okay to hide behind a screen and bully. So if someone want to say(sic) something nice, they should say it to them directly, not through an anonymous messaging app where people are constantly getting hurt and bullied.").

Lead Plaintiff-Appellee Carson Bride

On June 23, 2020, the Bride family, of Oregon, was struck by an unthinkable tragedy. *See* ER-21 (AC ¶ 10). 16-year-old Carson Bride took his own life after suffering months of cyberbullying on YOLO and LMK. *Id*. These messages included physical threats, obscene sexual messages and propositions, and other humiliating comments. *See* ER-50 (AC ¶ 90-91). Carson's efforts to find his tormentors on the anonymous app were futile: he asked the commenters to voluntarily S/U (swipe up) but the harassers remained hidden; he asked other classmates about the identity of commenters, but they had no way of knowing. *See* ER-51-52 (AC ¶ 96-98). On the night of his death, Carson's web search history shows that he was searching how to reveal YOLO usernames. *See* ER-52 (AC ¶ 100).

Two weeks after Carson's death, Carson's grieving parents Kristin and Tom Bride contacted YOLO on their "Contact Us" form and Customer Support page, writing about the cyberbullying that led to Carson's death and asking for the harassing users' identities to be revealed. *See* ER-53-55 (AC ¶¶ 105-117). Despite YOLO's promise to ban and reveal the identities of harassing and bullying users, YOLO did not respond. *Id*. Carson's parents then attempted to make contact through YOLO's law enforcement email address, but the message would not even transmit. *See id*. Through a professional contact, they then reached out personally to YOLO's founder, Gregory Henrion, but still received no response. *Id*.

On May 10, 2021, Carson's mother Kristin, along with the national nonprofit organization Tyler Clementi Foundation, filed this lawsuit against YOLO and two other defendants in the case. ER-16. Within 48 hours of filing the lawsuit, Snap Inc. ("Snap") suspended YOLO and LMK from Snapchat. ER-21-22 (AC ¶ 12). And on March 17, 2022, Snap announced that it would fully ban anonymous messaging apps like YOLO and LMK from its platform. *Id*. As Snap explained, "we believe some users" of "anonymous integrations" like YOLO and LMK "might be more prone to engage in harmful behavior — such as bullying or harassment — if they have the shroud of anonymity." *Id*.

Plaintiffs-Appellants Tyler Clementi Foundation, A.K., A.C., and A.O.

The Tyler Clementi Foundation brings claims as an organizational plaintiff on behalf of itself and its associated members (e.g., Youth Ambassadors). ER-90 (AC ¶ 268). The Foundation's mission and activi-

ties focus on educating parents, schools, and children about preventing cyberbullying and providing effective interventions in cyberbullying scenarios. The Foundation alleged that it diverted research and investigation resources specifically into the harms of anonymous apps due to their known dangers. ER-62-63 (AC ¶ 156). And because YOLO frustrated the organization's purpose of preventing cyberbullying, the Foundation and its associated members alleged that they were injured. *See* ER-32 (AC ¶ 36).

A.K., A.C., and A.O. joined the lawsuit and their claims were included in the Amended Complaint. A.K. is a minor child who used YOLO and was persistently harassed by those sending vicious anonymous messages. *See* ER-56-57 (AC ¶¶ 122-27). The anonymous users encouraged her to commit suicide, sent death threats, and made body shaming remarks. *Id.* Relying on YOLO's statement that it would reveal harassers' identities, A.K. sent requests to YOLO to reveal her bullies' identities but YOLO ignored her request. *Id.*

A.C. was only 13 years old when she used YOLO and suffered from harassing messages. The anonymous messages encouraged her to commit suicide while she was grieving the recent death of her brother, and included body-shaming comments. *See* ER-57-59 (AC ¶¶ 129-140). A.C.'s frustrations grew as she could not find a way to discover the identities of the vicious YOLO users who were protected by YOLO's anonymity product. *Id.*

A.O. is a minor child who used YOLO and was harmed by harassing and bullying messages. *See* ER-59-60 (AC ¶¶ 141-48). The messages she received through YOLO included being called offensive names such as a "whore," sexual solicitation, and body-

shaming remarks. *Id.* A.O. was unable to discover the identities of the senders of those messages because they were protected by YOLO's anonymity product. *Id.*

Complaint

Plaintiffs-Appellants brought a national class action representing a class and subclasses of individuals who used YOLO and were similarly harmed. In the Complaint, Plaintiffs-Appellants asserted (1) strict product liability based on a design defect; (2) strict product liability based on a failure to warn; (3) negligence; (4) fraudulent misrepresentation; (5) negligent misrepresentation; (6) unjust enrichment; (7) violation of the Oregon Unlawful Trade Practices Act; (7) violation of the New York General Business Law § 349; (8) violation of the New York General Business Law § 350; (9) violation of the Colorado Consumer Protection Act; (10) violation of the Pennsylvania Unfair Trade Practices Law; (11) violation of the Minnesota False Statement in Advertising Act; and (12) violation of California Business and Professions Code §§ 17200 & 17500. *See* ER-24-30 (AC ¶¶ 20-30, 178-322).

Throughout this brief, the strict liability, negligence, and state statutory claims that relate to YOLO's inherently dangerous and defectively designed product are referred as "Products Liability Claims"; the claims related to YOLO's failure to warn users of the danger of their products are referred to as "Failure to Warn claims"; and the claims asserting that YOLO made fraudulent misrepresentations and false advertising are referred to as the "Misrepresentation and False Advertising Claims."

The Complaint made clear that it does not "seek to hold Yolo or Lightspace liable as the publisher or speaker of the content provided by third parties within the meaning of Section 230. Instead, the plaintiffs seek to hold the defendants liable for their own conduct, namely their negligent design of products that would cause foreseeable harm that outweighs the utility of their products, their own failure to warn of the danger of their products, and their own misrepresentations about the specific steps they would take to stop harassment and bullying of users." ER-23 (AC ¶ 17).

The Complaint further explained each of the claims and underlying duty as follows:

> *One of the duties that Yolo [] violated springs from the duty to take reasonable measures to design a product that is more useful than it was foreseeably dangerous. By simply removing the element of anonymity, Yolo []could have complied with this duty to design a reasonably safe product. It could have provided the same messaging tools—such as the ability of users to send polling requests to each other—without monitoring or changing the content of the messages. Likewise, Yolo [] could have complied with their duty to warn users (and users' parents and guardians) of the danger of anonymous messaging without monitoring or changing the content of users' messages. And Yolo [] could have complied with their duties under the common law and state statutory law not to make false, deceptive, or misleading statements simply by accurately describing their own products, services, and*

business practices, or by not making such statements at all.

ER-23-24 (AC ¶ 18). The Complaint specified that YOLO's anonymity product itself inherently causes harm and psychological anxiety independent of the content of the messages sent using the product. For example, Carson's continued and painstaking efforts to investigate his harassers' identity until moments before his death demonstrates the tormenting anxiety and pressure that YOLO's anonymity feature imposed on him. *See* ER-52 (AC ¶ 97). Anonymity hinders victims from appropriately handling the content of messages because it deprives them of any means of confronting the perpetrators or assessing the possible reasons for those messages, and this leaves a sense of unresolved anger and harm especially in developing teenagers that makes it impossible for guardians, schools, or law enforcement to intervene. *See* ER-39 (AC ¶ 56).

Moreover, YOLO's false statement creates a new type of harm that is separate from the third-party messages. This includes the level of stress and frustration that was experienced by Carson as he was searching online for means to reveal his YOLO bullies on the night prior to his death. *See* ER-51 (AC ¶ 94). Similarly, A.K., A.O., and A.C. were harmed when they all relied upon YOLO's statement that harassing users will be unmasked, and later their requests to reveal the identities of harassers were ignored. *See* ER-57-60 (AC ¶¶ 122-48).

District Court's Decision

In a decision dated January 10, 2023, the District Court held that "Section 230 immunizes Defendant[-

Appellee] from Plaintiffs' claims in their entirety" and dismissed the Complaint with prejudice. ER-15. The District Court reasoned that while Plaintiffs-Appellants' claims "frame user anonymity as a defective design feature of Defendants' applications, Plaintiffs fundamentally seek to hold Defendants liable based on content published by anonymous third parties on their applications. Accordingly, the court finds Plaintiff's theories of liability treat Defendants as a "publisher" within the meaning of Section 230." ER-9. The lower court further held that YOLO's decision to allow or prevent users from using anonymity tools are "decisions about the structure and operation of a website are content-based decisions" under Section 230." ER-10. The District Court added that the claims here are not distinguishable from "*Dyroff* given the Ninth Circuit ultimately concluded that the defendant was entitled to immunity under the plain terms of Section 230 and our case law as a publisher of third-party content because the plaintiff could not and did not plead that the defendant required users to post specific content, made suggestions regarding the content of potential user posts, or contributed to making unlawful or objectionable user posts." ER-10 (internal citations and quotations omitted).

Distinguishing this case from the Ninth Circuit precedent in *Lemmon*, the District Court held:

> Though Plaintiffs seek to characterize anonymity as a feature or design independent of the content posted on Defendants' applications, the theories underlying Plaintiffs' claims essentially reduce to holding Defendants liable for publishing content created by third parties that is allegedly

> harmful because the speakers are anonymous. Imposing such a duty would "necessarily require [Defendants] to monitor third-party content," cf. *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019), e.g., in the form of requiring Defendants to ensure that each user's post on their applications is traceable to a specifically identifiable person.

ER-11. With regard to the Misrepresentation and False Advertising Claims, the District Court held that "those claims are still predicated on content developed by those third parties. Had those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable." ER-12. Dismissing the Failure to Warn Claims, the lower court found them barred by the CDA because "Plaintiffs' theory would require the editing of third-party content, thus treating Defendants as a publisher of content. Accordingly, *Internet Brands* is inapposite on this issue." ER-14.

PROCEDURAL HISTORY

Representing Carson Bride's estate, Carson's mother Kristin Bride brought the initial Complaint on May 10, 2021, against Defendant-Appellant YOLO and former Defendants Snap, Inc., and Lightspace Inc. in the Northern District of California. ER-113 (Dkt. 1.) The venue was transferred to the Central District of California on August 18, 2021. ER-118-19 (Dkts. 49-50 & 53.). Plaintiff filed the First Amended Complaint on June 27, 2022. ER-125 (Dkt. 113). YOLO submitted a motion to dismiss on October 6,

2022 ER-128 (Dkt. 127). The lower court heard oral argument on January 5, 2023. ER-128 (Dkt. 141). A decision granting the motion to dismiss with prejudice was issued on January 10, 2023. ER-128 (Dkt. 142). Plaintiffs-Appellants timely appealed on February 9, 2023. ER-128 (Dkt. 143). Claims were withdrawn and dismissed against Defendant-Appellant Lightspace on August 11, 2023. *See* Unopposed Mot. To Dismiss Party, Dkt. 22.

STATEMENT OF THE ISSUES

Whether Section 230 of the Communications Decency Act allows Plaintiffs-Appellants to bring claims for strict product liability, negligence, failure to warn, and misrepresentation claims based on a social media company's action of designing an app that lacks its own stated safety measures.

Whether Plaintiffs-Appellants adequately plead facts that YOLO violated strict product liability, negligence, failure to warn, and misrepresentation laws by their own conduct and statements, independent of third-party communications.

Whether the District Court erred by adopting a but-for standard in determining whether "treatment of publisher or speaker" prong of the CDA provision is satisfied.

Whether the District Court erred by failing to distinguish the duty derived from each claim brought by the Plaintiffs-Appellants in this case.

Whether the District Court erred by forcing factual inferences against Plaintiffs-Appellants in deciding a motion to dismiss.

STANDARD OF REVIEW

The standard of review over a district court's motion to dismiss complaint under Rule 12(b)(6) of the Federal Rules of Civil Procedure is reviewed de novo. *See Curtis v. Irwin Indus., Inc.*, 913 F.3d 1146, 1151 (9th Cir. 2019). In reviewing the dismissal of a complaint, this Court accepts "all factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Rowe v. Educ. Credit Mgmt. Corp.*, 559 F.3d 1028, 1029–30 (9th Cir. 2009) (internal quotation marks omitted).

SUMMARY OF ARGUMENTS

The dispositive question in this appeal is whether the Communications Decency Act, 47 U.S.C. § 230 (c)(1) ("CDA" or "Section 230"), bars Plaintiffs-Appellants' claims when all factual inferences are drawn in their favor. The text, history, and stated policies of the CDA makes clear that the law shields internet companies only when a plaintiff's claim faults the defendant for information provided by others, not for any claims targeting the companies' own conduct. Moreover, the CDA was enacted to protect Good Samaritans who sought to protect children from harmful contents and encourage removal of harmful contents. The District Court's decision contravenes the plain text of the statute and all of the stated policy goals therein.

Moreover, the District Court's dismissal of the Plaintiffs-Appellants' complaint is unsupported by this Court's precedents. In *Barnes v. Yahoo!, Inc.*, this Court created a three-pronged test for determining whether an internet company may be exempt from

liability under Section 230. 570 F.3d 1096, 1100 (9th Cir. 2009). Under this test, immunity from liability exists for "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider." *Id.* at 1100-01.

Here, the first prong is undisputedly met, because Defendant-Appellee is the developer of a mobile application that allows users to communicate with one another. Regarding the second prong, however, the District Court erred by foregoing an analysis of whether the duty in each of Plaintiffs-Appellants' claims arise from the internet company's role as a publisher or a product manufacturer, instead adopting a "but-for" test that has already been rejected by this Court. As for the third prong, the District Court further erred by ignoring facts alleging that Defendant-Appellee was responsible as an information content provider, and failed to draw all factual inferences in Plaintiffs-Appellants' favor when it found that YOLO was a content-neutral tool that did not encourage any unlawful or objectionable content. The District Court further erred by dismissing Plaintiffs-Appellants' failure to warn and misrepresentation/false advertising claims, which are solely based on Defendants' own conduct and statements.

ARGUMENT

A. The Lower Court's Decision Contradicts the Statutory Text, History, and Purpose of the Communications Decency Act

"In interpreting a federal statute, the Court must first determine whether the language is clear and unambiguous, and if so, apply it as written." *Thrifty Oil Co. v. Bank of Am. Nat. Trust & Sav. Ass'n*, 322 F.3d 1039, 1057 (9th Cir. 2003) (citing *Conn. Nat. Bank. v. Germain*, 503 U.S. 249, 253–54 (1992)). The Court considers "not only the bare meaning of the critical word or phrase but also its placement and purpose in the statutory scheme." *Id.* (quoting *Holloway v. United States*, 526 U.S. 1, 6 (1999)).

1. CDA Shields Internet Companies Only When the Claims Treat Them as Publishers and Speakers of Information

By its plain text, CDA Section 230(c)(1) protects interactive computer services only to the extent that they are treated "as the publisher or speaker" of information:

> "(1) 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."

47 U.S.C. § 230 (c)(1).

The purposeful use of the phrase "treated as the publisher or speaker," by its plain meaning, "cuts off liability only when a plaintiff's claim faults the defendant for information provided by <u>third parties</u>."

Lemmon v. Snap, Inc., 995 F.3d 1085, 1093 (9th Cir. 2021) (emphasis added) (citing 47 U.S.C. § 230 (c)(1)).

If Congress intended to provide a comprehensive and broad immunity provision, it could have simply replaced "be treated as the publisher or speaker of" with "be held responsible for" when drafting the provision. However, as this Court noted, the CDA was enacted in response to *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995*),* in which the court found an online service provider "Prodigy" responsible for libelous content posted on its message board. Prodigy voluntarily deleted some of the messages but was held liable for the messages it failed to delete because the court deemed it to be a publisher of those messages. Hence, as the legislature explained, "[o]ne of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers . . . as publishers or speakers of content that is not their own because they have restricted access to objectionable material." H.R. Rep. No. 104-458 (1996) (Conf. Rep.), *as reprinted in*, 1996 U.S.C.C.A.N. 10; *accord Roommates.com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008). As seen here, the aim of the CDA was to prevent liability only in a narrow context—where an internet company is sought to be held liable under publisher-based claims in the course of removing objectionable content.

Aligned with this reading, the Seventh Circuit clarified that "§ 230(c)(1) is not a comprehensive grant of immunity for third-party content. Instead, that subsection precludes liability only where the success of the underlying claims requires the defendant to be

considered a publisher or speaker of that content. But § 230(c)(1) may not necessarily preclude liability if the underlying claims identify the interactive computer service's own content as objectionable." *Webber v. Armslist LLC*, 70 F.4th 945, 957 (7th Cir. 2023) (emphasis added).

Here, the District Court reached beyond the text of the statute when it dismissed Plaintiffs-Appellants' claims, oversimplifying the claims as predicated on YOLO's publication of third-party content, even though the claims were based on the internet company's own conduct as a product developer: designing YOLO's anonymity feature without reasonable safety, failing to warn about the manifestation of harassment and bullying, and making false promises of safety to young consumers about the product . *See infra*, at 32.

2. The CDA is a Good Samaritan Statute that Protects Good Faith Effort to Remove Offensive Material

The purpose of the CDA is written in its title: "Protection for Good Samaritan Blocking and Screening of Offensive Material." 47 U.S.C. § 230. It extends to "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." 47 U.S.C. § 230(c)(2)(A) (emphasis added).

Congress also stated in the CDA that "[i]t is the policy of the United States—

(1) to promote the continued development

> of the Internet . . . (2) to preserve the vibrant and competitive free market that presently exists for the Internet . . . (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material . . . "

47 U.S.C. § 230(b) (emphasis added). These provisions demonstrate that Congress sought to "immunize the *removal* of user-generated content, not the *creation* of content." *Roommates.com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008) (emphasis in original). This limitation of liability had the dual purpose of "promot[ing] the free exchange of information and ideas over the Internet and . . . encourag[ing] voluntary monitoring for offensive or obscene material." *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003).

Allowing internet companies that host third-party content to be free from liability, regardless of whether they are making good-faith efforts to prevent harm as "Good Samaritans," contradicts Congress's stated aim in enacting the CDA. Here, the Complaint alleged that YOLO designed an app with anonymity features—knowing these features would induce harassing and harmful messages—and assured consumers by representing that it had safety measures in place, without actually implementing them. *See* ER-66 (AC ¶ 65). YOLO's conduct is completely inconsistent with that of a "Good Samaritan." YOLO drew in vulnerable minor users with its attractive anonymity feature, gave a false sense of security to guardians, bystanders, and users with empty promises and inef-

fective guardrails, and now attempts to exploit the CDA shield.

Affording immunity in this case defies every policy goal explicitly stated in the CDA. By allowing companies to release unsafe products and lie to the public obstructs, rather than "promote[s,] the continued development of the Internet." *See* 47 U.S.C. § 230(b). Such precedent would infect the "vibrant and competitive free market that presently exists for the Internet" by creating a race to the bottom. *See id*. Immunity under these facts also incentivizes bad actors and market participants by rewarding instead of punishing false advertising and deceptive statements. And, of course, immunity provides a perverse incentive for companies to do nothing in the face of imminent danger, which runs afoul of the goal of encouraging the "development and utilization of blocking and filtering technologies." *See id*.

Unless reversed, this precedent will permit companies to develop and profit from all kinds of dangerous and deceptive products. Currently, too many internet companies profit from feeding harmful and egregious content to young users, from unrealistic beauty standards to the sale of child pornography, sale of illicit and fatal drugs, and promotion of gun violence and terrorism. Left to their own devices, social media apps will be designed to increase the publication and consumption of addictive, salacious, and dangerous content driven by short term market incentives for companies to "race to the bottom." Technology already exists that would allow a suite of unthinkably horrifying conduct if companies were unrestrained in how they implement it. Imagine, for example, deepfake and generative artificial intelligence

tools used by children on social media enabling creation of images that depict violence, nudity, and other harmful contents just by typing in a prompt; rigged location sharing technology or hacking tools that are used over social media to bypass safety guidelines set by law enforcement and guardians, combined with lucrative ingredients like anonymity, lack of age-verification, and data privacy intrusions. Should the District Court's precedent stand, individuals and companies would use those technologies to exploit social unrest, mistrust, and even violence for short-term profit, all while enjoying broad protection under the CDA. Ultimately, young users, parents, and students alike who are victims of these unchecked technologies are not only lied to but are left without any recourse when they are harmed. Therefore, based on the plain text of the statute and the policy purposes expressed by Congress, this Court must reverse the District Court's decision and allow Plaintiffs-Appellants' claims to proceed.

B. The District Court Erroneously Used a "But-For" Test in Reviewing *Barnes*' Second Prong, And Failed to Analyze the Duty Underlying Each State Law Claim

The District Court erred in deciding that the second prong of *Barnes* was met by adopting and applying a "but-for" publication test – that CDA immunity applies if a cause of action would not be cognizable "but-for" content from a third party. *See* ER-12 ("Had those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable.").

The Ninth Circuit and other Circuit Courts have consistently rejected this "but-for" test. *See, e.g.*, *HomeAway.com*, 918 F.3d at 682 ("*Internet Brands* rejected use of a but-for test that would provide immunity under the CDA solely because a cause of action would not otherwise have accrued but for the third-party content."). In *Doe v. Internet Brands, Inc.*, this Court ruled that a "but-for" test would "stretch the CDA beyond its narrow language and its purpose." 824 F.3d 846, 853 (9th Cir. 2016). There, the plaintiff created content for her model profile and published it on the internet website "Model Mayhem." She was then raped by two perpetrators who used the internet platform to lure female victims to assault and record pornography for sale and distribution. *Id.* at 848. The owner of the website was informed that the two perpetrators were using the website but did not warn users, including the plaintiff. *Id.* Upon these facts, this Court decided that Section 230 immunity did not apply to the plaintiff's failure to warn claims, and in its reasoning, expressly rejected a "but-for" test:

> To be sure, Internet Brands acted as the "publisher or speaker" of user content by hosting Jane Doe's user profile on the Model Mayhem website, and that action could be described as a "but-for" cause of her injuries. Without it, Flanders and Callum would not have identified her and been able to lure her to their trap. But that does not mean the failure to warn claim seeks to hold Internet Brands liable as the "publisher or speaker" of user content. Publishing activity is a but-for cause of just about everything Model Mayhem is involved in. It is an internet

> publishing business. Without publishing user content, it would not exist.

Doe v. Internet Brands, Inc., 824 F.3d 846, 853 (9th Cir. 2016). Instead, this Court reiterated its decision in *Barnes*, wherein it examined the duty invoked by each of the claims, and differentiated a publisher's duty versus a non-publisher's duty for determining whether to afford CDA immunity:

> In [Barnes] we affirmed the dismissal of a claim for negligent undertaking as barred under the CDA . . . but we reversed the dismissal of a claim for promissory estoppel under Oregon law. The publication of the offensive profile posted by the plaintiff's former boyfriend was a "but-for" cause there, as well, because without that posting the plaintiff would not have suffered any injury. But that did not mean that the CDA immunized the proprietor of the website from all potential liability. . . . "we must be careful not to exceed the scope of the immunity provided by Congress." Congress could have written the statute more broadly, but it did not.

Id. (emphasis added) (quoting *Roommates*, 521 F.3d at 1164 n.15.)

In *Barnes v. Yahoo!, Inc.*, the plaintiff brought negligence and promissory estoppel claims against Yahoo for failing to remove her ex-boyfriend's posts containing nude photographs of her. This Court's decision parsed the negligence from the promissory estoppel claims by examining whether the duty of Yahoo to remove third-party content derives from the internet

company's role as a publisher or a party to a contract. This Court found that in the negligence claims, the duty arose from Yahoo's role as a publisher, but in the promissory estoppel claim, the duty arose from Yahoo's contractual obligation to remove the injurious content. *Id.* at 1107-07 ("Barnes does not seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promisor who has breached."). This Court further explained that "[c]ontract 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." *Id.* at 1107 (emphasis added).

In this case, the products liability, negligence, and state consumer protection claims seek to hold YOLO liable for failing to take actions to increase the safety of its consumers from the harms of cyberbullying, such as removing offensive users from its platform or revealing their identities. Like *Barnes*, this duty does not derive from YOLO's publishing conduct, but from YOLO's role as a developer, seller, and advertiser of its anonymous messaging product, where it unequivocally expressed that it would remove or reveal the individuals who harass or bully others on its platform. Applying *Barnes* to this case, even if YOLO's removal or revealing identities of individuals happens to coincide with YOLO's duty as a publisher, this does not activate CDA immunity because Plaintiffs-Appellants' claims rely upon a duty – the duty to make reasonably safe products – that is separate from YOLO's publisher duty. *See id.*

Instead, the lower court departed from *Barnes* by ruling that CDA immunity applies because Plaintiffs-

Appellants' claims require YOLO to monitor third-party content by ensuring that each post can be traceable to the sender:

> Though Plaintiffs seek to characterize anonymity as a feature or design independent of the content posted on Defendants' applications, the theories underlying Plaintiffs' claims essentially reduce to holding Defendants liable for publishing content created by third parties that is allegedly harmful because the speakers are anonymous. Imposing such a duty would "necessarily require [Defendants] to monitor third-party content . . . in the form of requiring Defendants to ensure that each user's post on their applications is traceable to a specifically identifiable person.

ER-11. The District Court's reasoning above failed to even attempt to identify the duty in each of Plaintiffs-Appellants' claims, despite this Court's holding in *HomeAway.com* 918 F.3d 676 (9th Cir. 2018). In *HomeAway*, the city of Santa Monica passed an ordinance requiring internet platforms that host rental properties to ensure that the properties listed are licensed and listed on the City's registry before completing any booking transactions. The hosting platform, HomeAway argued that CDA granted immunity from suit under the ordinance because the property listings published on its platform were third party content.

In holding that CDA does not apply, this Court first rejected the "but-for" test:

> We do not read Internet Brands to suggest

> that CDA immunity attaches any time a legal duty might lead a company to respond with monitoring or other publication activities. It is not enough that third-party content is involved; Internet Brands rejected use of a "but-for" test that would provide immunity under the CDA solely because a cause of action would not otherwise have accrued but for the third-party content.

HomeAway.com, 918 F.3d at 682 (quoting *Internet Brands*, 824 F.3d at 853) (emphasis added).

This Ninth Circuit then instructed that the reviewing court should examine each claim for "what the duty at issue actually requires: specifically, whether the duty would necessarily require an internet company to monitor third-party content." *Id*. (emphasis added) (quoting *Internet Brands*, 824 F.3d at 851, 853).

The *Homeaway.com* court found that the underlying duty imposed by the ordinance could have been discharged without necessarily changing the content of users' listings on the website. Further, this Court reasoned that:

> [e]ven assuming that removing certain listings may be the Platforms' most practical compliance option, allowing internet companies to claim CDA immunity under these circumstances would risk exempting them from most local regulations and would, as this court feared in Roommates.com, 521 F.3d at 1164, "create a lawless no-man's-land on the Internet." We hold that the Ordinance is not "inconsistent" with the CDA, and is therefore not expressly preempted by its terms.

HomeAway.com v. City of Santa Monica, 918 F.3d 676, 683 (9th Cir. 2018).

Similar to *Homeaway.com*, Plaintiffs-Appellants here have alleged that Defendant-Appellee's duty underlying the products liability claims (duty to make a reasonably safe product), misrepresentation/false advertising claims (duty not to make false, deceptive, or misleading statements), and failure to warn claims (duty to warn) can be discharged without removing or editing content:

> By simply removing the element of anonymity, Yolo and Lightspace could have complied with this duty to design a reasonably safe product. It could have provided the same messaging tools—such as the ability of users to send polling requests to each other—without monitoring or changing the content of the messages. Likewise, Yolo and Lightspace could have complied with their duty to warn users (and users' parents and guardians) of the danger of anonymous messaging without monitoring or changing the content of users' messages. And Yolo and Lightspace could have complied with their duties under the common law and state statutory law not to make false, deceptive, or misleading statements simply by accurately describing their own products, services, and business practices, or by not making such statements at all.

ER-23 (AC¶ 18).

Other circuit courts have joined in rejecting a "but-for" test, instead opting to examine the duty underlying each specific claim alleged for purposes of

CDA immunity. For example, in *Henderson v. Source For Pub. Data, L.P.*, 53 F.4th 110, 122 (4th Cir. 2022), the court reasoned that the CDA does not bar claims brought under the Fair Credit Reporting Act against companies that publish consumer credit information online:

> Most of what Public Data allegedly does, after all, is publish things on the internet. That means that publishing information is one but-for cause of these FCRA claims against Public Data. If Public Data is a "consumer reporting agency" subject to FCRA liability, it is one because it is the publisher or speaker of consumer report information. Yet that alone is not sufficient, as we do not apply a but-for test. *See Erie Ins.*, 925 F.3d at 139-140; HomeAway.com, 918 F.3d at 682. We must instead examine each specific claim.

Henderson, 53 F.4th 110, 123 (4th Cir. 2022) (emphasis added).

In this case, the District Court incorrectly concluded that Plaintiffs-Appellants' claim was reduced to publisher liability because it would require YOLO to "monitor third-party content . . . in the form of requiring Defendants to ensure that each user's post on their applications is traceable to a specifically identifiable person." ER-10. This conclusion contains a logical error: a product liability claim does not always require a duty to monitor, and a duty to monitor claims can stem from non-publisher liability. As held by this Court in *Lemmon*, "The duty to design a reasonably safe product is fully independent of [a defendant's] role in monitoring or publishing third party content."

995 F. 3d at 1092. That a defendant allows "its users to transmit user-generated content to one another does not detract from the fact that [a plaintiff] seek[s] to hold [the defendant] liable for its role in violating its distinct duty to design a reasonably safe product." *Id*. This Court in *Barnes* also explained that the CDA does not bar promissory estoppel claims where a duty to monitor is generated by contract liability where an internet company is a party to a contract. *Barnes*, 570 F.3d at 1107 ("[c]ontract 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.").

The District Court's opinion also forces factual inferences not contemplated or asserted in the pleadings when it noted that the Plaintiffs-Appellants' claim requires monitoring the form of ensuring that each user's post is traceable to an identifiable person. *See* ER-11. As alleged in the Amended Complaint, YOLO users are already traceable and identifiable, because they can either remove their anonymity by voluntarily "swiping up" or, as YOLO advertised, by YOLO removing the user's anonymity mode. ER-27-28 (AC ¶ 26). Hence, YOLO could have complied with its duty under products liability law by, among other means, simply allowing receivers of anonymous messages to remove their sender's anonymity and reveal their identity. In its opinion, the District Court did not accept the Complaint's factual allegations as true and draw all factual inferences in Plaintiffs-Appellants' favor – which it was required to do at the motion to dismiss stage. *See* Fed. R. Civ. P. 12; *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1090 (9th Cir. 2021) (holding that

a "complaint will survive at this stage if it states 'a plausible claim for relief'").

Therefore, the District Court's adoption of the "but-for" rule in reviewing the second prong of *Barnes* is already rejected by this Court, and its failure to parse out the duty underlying each of Plaintiffs-Appellants' claims, led to an erroneous conclusion. Its reasoning conflicted with binding precedent of this Circuit, and its holding should therefore be reversed.

C. The District Court Failed to Analyze Defendant-Appellee's Own Conduct and Role As an Information Content Provider Under *Barnes*' Last Prong

"By its plain terms, and as the last part of the *Barnes* test recognizes, 230(c)(1) cuts off liability only when a plaintiff's claim faults the defendant for information provided by third parties." *Lemmon*, 995 F.3d 1085, 1093 (9th Cir. 2021) (emphasis added) (citing 47 U.S.C. § 230(c)(1)). Therefore, internet companies are not shielded from liability where (1) they create or develop their own internet content, or (2) the plaintiff's claims are predicated on the internet companies' "own acts." *Id.*; *see also In re Apple Inc. Litig.*, 625 F. Supp. 3d 971, 995 (N.D. Cal. 2022) ("the history of section 230 does not support a reading of the CDA so expansive as to reach a websites-generated message and functions") (citing *Gonzalez v. Google LLC*, 2 F.4th 871, 913 (9th Cir. 2021) (Berzon, J., concurring, opining that targeting recommendations are not traditional publisher activity); *Force v. Facebook, Inc.*, 934 F.3d 53, 76 (Katzmann, C.J., concurring in part and dissenting in part, opining that Facebook's friend suggestion algorithm is not a publisher activity).

This Court has held that a website can be liable as an information content provider if they "create or develop" content "by making a material contribution to [its] creation or development," thus bringing the company outside the CDA's protections. *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1269 (9th Cir. 2016) (citing *Gonzalez v. Google LLC*, 2 F.4th 871, 892 (9th Cir. 2021)). Thus, where a website's design is responsible for what makes the displayed content allegedly unlawful, it materially contributes to the content and loses immunity under CDA. *Gonzalez*, 2 F.4th at 892. On the other hand, where a website design is merely a neutral tool, it does not meet this "material contribution" test.

Illustrating the material contribution in *Roommates.com*, 521 F.3d 1157, 1161 (9th Cir. 2008) (*en banc*), this Court decided that a roommate-matching website had materially contributed to violations of the Fair Housing Act that occurred on the website, and thus, Section 230 immunity would not apply. The website in *Roommates.com* was designed to prompt and require users to input protected class information (such as sexual orientation and number of children) and developed a search system that allowed users to filter individuals using protected class characteristic. 521 F.3d at 1167. Accordingly, this Court found that the website's prompts and search functions were not neutral tools. These functions materially contributed to content and conduct on the website that were unlawful and discriminatory.

Echoing the reasoning in *Roommates.com*, this Court in *Lemmon v. Snap* held that CDA does not shield defective design claims when a product's design choice encourages a particular user behavior that is

dangerous. 995 F.3d at 1093 ("internet companies remain on the hook when they create or develop their own internet content. . . . and to the extent they are "'responsible . . . in part, for the creation or the development of' the offending content" on the internet.") (citing *Roommates.com*, 521 F.3d at 1162). This Court found that even though Snap, Inc. is a publisher, the fact that it developed Snapchat's "Speed Filter and the incentive system [which] then supposedly worked in tandem to entice young Snapchat users to drive at speeds exceeding 100 MPH" exposed Snap to liability for negligent design claims. 995 F.3d at 1091-92.

In contrast, in *Carafano*, this Court considered to what extent an online dating site can be legally responsible when an ill-intentioned user created a libelous dating profile impersonating actress Christianne Carafano and disclosed her personal contact information. *Carafano*, 339 F.3d at 1121-22. Carafano subsequently brought claims against the dating site for invasion of privacy, misappropriation of her right of publicity, defamation, and negligence. *See id*. The Ninth Circuit determined that the website's functions were neutral tools because the website did not encourage the posting of defamatory content, but merely provided a means for users to publish the profiles they created themselves. *Id*. This Court found that the design of the online dating site's profile "contents were left exclusively to the user," who can select the options for questionnaire and provide an essay answer. *Id.* at 1124. This Court noted that the defendant company was not responsible "even in part, for associating certain multiple-choice responses with a set of physical characteristics, a group of essay answers, and a photograph." *Id*. Under those circumstances, the court

concluded that the dating site could not be considered an "information content provider." *Id.*

In *Dyroff v. Ultimate Software Grp., Inc.*, this Court concluded that a website was entitled to CDA immunity where it operated a message board that had "features and functions, including algorithms, to analyze user posts . . . and recommend other user groups." 934 F.3d 1093, 1098-99 (9th Cir. 2019). Using these features, the plaintiff in *Dyroff* interacted with another user on the website, which ultimately resulted in a fatal and illegal drug sale. *Id.* at 1098. The Ninth Circuit found that the website's features, including chat group recommendation, notifications, and the non-collection of identification credentials (pseudonymity), did not amount to the defendant assisting in creating the offending content, because those features were merely neutral tools "meant to facilitate the communication and content of others." *Id.*

In *Gonzalez v. Google LLC*, families of deceased victims of an ISIS terrorist attack brought claims against Google under the Anti-Terrorism Act (ATA), 18 U.S.C.S. § 2333, alleging that Google was directly and secondarily liable for allowing ISIS to post content communicating the group's support for terrorism by publishing, recommending, and providing such content on the social media platforms. 2 F.4th 871 (9th Cir. 2021), *rev'd on other grounds*, 598 U.S. __ (2023). There, this Court reviewed the factual allegations regarding Google's algorithms to determine whether Google prompted users to post unlawful content. This Court found that the algorithm behind Google's search engine – which allegedly selects particular content for a user based on the user's own inputs – would be considered a content-neutral tool because it does not

"provide any encouragement to perform illegal searches or to publish illegal content." *Id.* at 896.

Threading this Court's decisions in the above cases, whether CDA immunity applies turns on whether the operative pleading alleges that the internet company's tool or product at issue is content-neutral. Content neutrality can be characterized in different ways, but it does not simply exist where the platform can be used in both lawful and unlawful ways. If that were the standard, then internet companies would be required to maintain policies ensuring that there be no content moderation whatsoever, which defies the very purpose of the CDA. And such a standard would be incoherent with this Court's holdings in *Lemmon* and *Roommates.com*, because the tools at issue in those cases were available to third-parties who used the tools for dangerous, unlawful, and/or discriminatory ways, just as much as they were available to third-parties who used them for innocuous purposes.

Rather, as made clear by this Court's precedents, a tool is "content-neutral" if it does not impact the substance of the created content. If a user would feel obliged to change the content of the speech based on the way that the tool is designed – e.g., requiring protected class information be stated in a profile questionnaire (*Roommates.com*), or a speed filter designed for car racing (*Lemmon*) – then it is not content-neutral. On the other hand, a profile questionnaire where users have wide discretion to choose the information to display on their profile (*Carafano*) and a blank search engine box that allows a user to input a search term to provide responsive content via an algorithm (*Gonzalez*) was found not contribute to the development of the offending content itself.

In this case, the District Court erred by ignoring facts alleging that the Defendant-Appellee's product design (anonymity tool) altered the way that minor users created and published their content on the app in a way that made it dangerous and unlawful, whereas without the tool, they would not have created the same content. *See* ER-9 (" . . . the plaintiff could not and [did] not plead that [the defendant] required users to post specific content, made suggestions regarding the content of potential user posts, or contributed to making unlawful or objectionable user posts.").

Contrary to the District Court's finding, the Amended Complaint's allegations demonstrate how YOLO's product's design choice encouraged dangerous user behavior:

- ER-18-19 (AC ¶ 3): anonymous online communications pose a significant danger to minors, including by increasing the risk of bullying and other antinormative behavior and amplifying the negative feelings of victims . . . Prior anonymous apps were "vulnerable to being used to spread hate speech and bullying.
- ER-44-45 (AC ¶ 71): (YOLO customer review) (e) . . . At a time when suicide is the number 1 killer of teens in America, we definitely don't need apps like this where bullied haters can hide behind a screen . . . (h) . . . it's teaching our youth that it's okay to hide behind a screen and bully. So if someone want to say something nice, they should say it to them directly, not through an anonymous messaging app where people are constantly getting hurt and bullied.

- ER-52 (AC ¶ 97): Do you know who is sending me all these sus(picious) YOLOs. Whenever I do one I only get people either trying to catfish me or bait me into saying dumb (things) or whatever . . . I guess I understand like a bit of sus(picious) shit every once in a while but it [is] my entire inbox of YOLO's.

Instead, the lower court ruled that this case is indistinguishable from *Dyroff*, without even attempting to give due attention to the detailed factual allegations:

> The court similarly finds that Dyroff is not materially distinguishable on the basis that the users of the application at issue in Dyroff remained pseudonymous while posting users of Defendants' applications remain anonymous . . .

ER-10 (quoting *Dyroff*, 934 F.3d at1099). Unlike the website Experience Project in *Dyroff*, where every user had a registered name attached to their posts, and every user remained pseudonymous (*id*. at 1100), YOLO was designed to give a one-sided privilege to keep the message sender anonymous, while the message receiver was identifiable. *See* ER-25, 39, 51 (AC ¶¶ 26, 56 & 96). This made targeted bullying inevitable, especially when unassuming teens would rely on YOLO's self-stated promise to reveal harassers' identities while using the app. The District Court further cited to other decisions where anonymity was a common component of a website but was designed and marketed with significant differences from YOLO, such as adult websites that "g[a]ve an option to anonymize email addresses." ER-10 (*citing Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116, 1124 (N.D. Cal. 2016) and

Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 20 (1st Cir. 2016)).

Recognizing that design choices of a medium can contribute to the message, Ninth Circuit pellucidly instructed that courts should avoid a "form over function" approach and inquire whether a website's tool contributed to the substance of the content. *See Roommates.com*, 521 F.3d at 1165-67. In *Roommates .com*, the Court noted that a questionnaire that lets users create their own criteria for identifying and choosing potential roommates (including criteria based on protected classes like race or sex) in a blank text box may be content-neutral, while a questionnaire that requires users to input protected class information and develops a search system that allowed users to filter individuals using the protected class characteristic contributed to the development of unlawful content. *Id*.

In *Gonzalez*, the Court acknowledged that Google's specific algorithms at issue were neutral but warned against categorically deeming algorithms as content-neutral: "we do not hold that machine-learning algorithms can *never* produce content within the meaning of Section 230. We only reiterate that a website's use of content-neutral algorithms, without more, does not expose it to liability for content posted by a third-party." *Gonzalez v. Google LLC*, 2 F.4th 871, 896 (9th Cir. 2021).

These Ninth Circuit precedents demonstrate the errors contained in the District Court's decision, which ignored facts alleging that the Defendant-Appellee's product design (anonymity tool) materially contributed to the unlawful content on YOLO. Therefore,

this Court should reverse the District Court's dismissal of this case.

D. Plaintiffs-Appellants' Failure to Warn Claims and Misrepresentation/False Advertising Claims Focus Solely on Defendant-Appellee's Own Conduct and Statements

Nothing in the text, purpose, legislative history, or courts' interpretation of the CDA allows internet companies to avoid liability for harms that derive from their own conduct and speech. The second prong of the test under *Barnes*, based on the text of the statute, is that the CDA would cut off liability where an internet company is treated as the "publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230 (c)(1); *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100 (9th Cir. 2009); *see also Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1093 (9th Cir. 2021).

Like the claims in *Lemmon v. Snap, Inc.*, the failure to warn and misrepresentation/false advertising claims alleged in the Amended Complaint "do[] not depend on what messages, if any, a [] user employing the [tool] actually sends. This is thus not a case of creative pleading designed to circumvent CDA immunity." 995 F.3d 1085, 1094 (9th Cir. 2021). Indeed, "the [CDA] was not meant to create a lawless no-man's-land on the Internet." *Roommates*, 521 F.3d at 1164. Hence, "Those who use the internet thus continue to face the prospect of liability, even for their neutral tools, so long as plaintiffs' claims do not blame them for the content that third parties generate with those tools." *Lemmon*, 995 F.3d at 1094 (quotation marks omitted).

The District Court's decision to dismiss the Plaintiffs-Appellants' failure to warn and misrepresentation/false advertising claims run counter to this Court's precedents. In *Doe v. Internet Brands*, 824 F.3d 846, 853 (9th Cir. 2016), this Court made clear that a plaintiff's failure to warn claims were not barred by the CDA where they are not based on any content posted on the website. Because the duty under the plaintiff's failure to warn claims did not require any action regarding third-party content posted on its site, the claims did not treat the defendant as a publisher or speaker of information. *See id.*; *see also A.M. v. Omegle.com, LLC*, 614 F. Supp. 3d 814, 820 (D. Or. 2022) (holding that the defendant failed to warn minor users about adult predators on the website, and that the website could have discharged the duty without having to "alter the content posted by its users—it would only have to change its design and warnings.").

Here, in dismissing Plaintiffs-Appellants' failure to warn claims, the District Court merely stated: "Plaintiffs' theory would require the editing of third-party content, thus treating Defendants as a publisher of content. Accordingly, *Internet Brands* is inapposite on this issue." *See* ER-13-14. The District Court's finding has no basis in the Amended Complaint, which alleged the contrary: "YOLO . . . could have complied with their duty to warn users (and users' parents and guardians) of the danger of anonymous messaging without monitoring or changing the content of users' messages." ER-23-24 (AC ¶ 18). Furthermore, the duty to warn only requires that YOLO create a proper warning about the proliferation of harassment and bullying, which they knew about through reports from consumers, or even provide individualized warnings.

ER-44-45 (AC ¶ 71). The District Court's decision is void of explanation as to why it inferred that the duty would require editing of any third-party content.

The District Court's dismissal of the misrepresentation/false advertising claim is similarly flawed. It reasoned that Plaintiffs-Appellants' misrepresentation and false advertising claims are still predicated on third-party content because "[h]ad those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable. . . . In sum, the accusation here is fundamentally that Defendants should have monitored and curbed third-party content." ER-12.

The District Court's logic fails for several reasons. First, the duty not to make false statement depends on YOLO's own affirmative statement to its users, in a conspicuous pop-up message: "YOLO is for positive feedback only. No bullying. If you send harassing messages to our users, your identity will be revealed." ER-42 (AC ¶ 65). The underlying duty not to make false statements is based on the factual allegation that Plaintiffs-Appellees read and relied upon this statement when they began using YOLO. *Id*. Hence, liability for misrepresentation/false advertising depends on YOLO's own promise to stop and reveal bullying and harassing users, not on YOLO's publishing conduct. Such conclusion conforms with this Court's precedent in *Barnes v. Yahoo!, Inc.*, where this court found that the CDA did not exempt Yahoo for liability under promissory estoppel claims because the duty arose from Yahoo's contractual obligation to remove the injurious content. *Barnes*, 570 F.3d at 1105-07; *see also id.* at 1107 ("[c]ontract 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.") (emphasis added).

Second, as discussed above in Section B, *supra* at 24, the District Court's reasoning contains exactly the kind of but-for standard that was outright rejected by Ninth Circuit precedent. *See* ER-12 ("[had] those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable . . . "). This type of reasoning would cause absurd results. For instance, if an internet company advertised that its messaging product charges users one dollar for each message sent, when in fact it charged two dollars per message, applying the District Court's reasoning, such false advertisements would still receive protection under the CDA because the harms would not have happened but-for the users' posting of messages. The District Court's conclusion effectively creates a "buyer beware" scenario without actually requiring the seller to warn the buyer, like in this case, allowing the seller to willfully lie to the buyer.

Third, the District Court erred in its conclusory finding that "[t]he accusation here is fundamentally that [Defendants] should have monitored and curbed third-party content." ER-12. YOLO could have discharged its duty not to make false statements to consumers simply by refraining from making false statements to consumers. *A.M. v. Omegle.com, LLC*, 614 F. Supp. 3d 814, 819 (D. Or. 2022) (holding that CDA did not apply to the design defect and failure to warn claims because the internet company could have

satisfied its duty simply by designing the product differently and changing its warnings, without any need to review, edit, or withdraw third-party content). YOLO could have truthfully stated that it lacked the capability or capacity to track harassers and bullies on its app, thereby putting minor users and their guardians on notice and allowing users to make informed decisions about either avoiding the app or implementing their own safety measures. *See* ER-23-24 (AC ¶ 18). ("Yolo . . . could have complied with their duties under the common law and state statutory law not to make false, deceptive, or misleading statements simply by accurately describing their own products, services, and business practices, or by not making such statements at all."). However, by notifying users that it would reveal harassers and bullies, YOLO misled its users.

And even assuming that monitoring third-party content is the most practical compliance option to discharge duties to warn and to not to make false and deceptive statements, that does not cover these claims under the CDA shield. *Lemmon v. Snap*, 995 F. 3d at 1092 ("The duty to design a reasonably safe product is fully independent of [a defendant's] role in monitoring or publishing third party content."); *HomeAway.com v. City of Santa Monica*, 918 F.3d 676, 683 (9th Cir. 2018) ("[e]ven assuming that removing certain listings may be the Platforms' most practical compliance option, allowing internet companies to claim CDA immunity under these circumstances would risk exempting them from most local regulations . . . ").

Therefore, this Court should reverse the District Court's decision to dismiss Plaintiffs-Appellants' failure to warn claims and misrepresentation/false adver-

tising claims, which are solely based on Defendant-Appellee's own conduct and statements, not of any third-party users.

CONCLUSION

For the above reasons, this Court should reverse the District Court's order dismissing Plaintiffs' claims against YOLO and remand for the case to move forward.

Dated: August 11, 2023

Respectfully submitted,

By: /s/ Juyoun Han
Eric M. Baum
Eisenberg & Baum, LLP
24 Union Square East, Penthouse
New York, NY 10003
(212) 353-8700

Attorneys for Plaintiffs-Appellants

PLAINTIFFS-APPELLANTS' OPPOSITION TO DEFENDANT APPELLEE YOLO TECHNOLOGIES, INC.'S MOTION TO STRIKE, (MARCH 8, 2024)

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

THE ESTATE OF CARSON BRIDE, BY AND THROUGH HIS APPOINTED ADMINISTRATOR KRISTIN BRIDE; A.K., BY AND THROUGH HER LEGAL GUARDIAN JANE DOE 1; A.C., BY AND THROUGH HER LEGAL GUARDIAN JANE DOE 2; A.O., BY AND THROUGH HER LEGAL GUARDIAN JANE DOE 3; TYLER CLEMENTI FOUNDATION, ON BEHALF OF THEMSELVES AND ALL OTHERS SIMILARLY SITUATED,

Plaintiffs-Appellants,

v.

YOLO TECHNOLOGIES, INC.,

Defendant-Appellee.

No. 23-55134

On Appeal from the United States District Court
for the Central District of California
The Honorable Fred W. Slaughter presiding
District Court Case No. 2:21-cv-06680-FWS-MRW

Juyoun Han
Patrick K. Lin
Eric Baum
EISENBERG & BAUM, LLP
24 Union Square East, Penthouse
New York, New York 10003
Telephone: (212) 353-8700

Attorneys for Plaintiffs-Appellants

{ Internal Table of Contents
and Table of Authorities Omitted }

LEGAL ARGUMENT

Contrary to Appellee's arguments stated in their motion to strike, (1) the "reveal and ban" feature has always been a basis for Appellants' product liability claim—*i.e.*, dangerous products that lack the safeguards ("reveal and ban")—alleged in both the Original Complaint and the First Amended Complaint ("FAC"); and (2) all of YOLO app's product features, taken as a whole, have always been at the core of the product liability claims.

1. The "Reveal and Ban" Feature Were Alleged for Both the Misrepresentation and Products Liability Claims

The Original Complaint and the FAC explicitly alleged that the YOLO app's "reveal and ban" feature contribute both to the misrepresentation and the product's inherently dangerous quality, because Appellee's inability to activate its safeguard ("reveal and ban") is connected to the danger and harm it caused.

The Appellee's argument that this argument was raised for the first time in the reply brief is blatantly incorrect. In the Original Complaint, under the section "FIRST CAUSE OF ACTION: STRICT LIABILITLY," the Appellants conspicuously alleged:

> Defendants' apps promoted cyberbullying and are designed to be inherently dangerous. LMK and YOLO are unable or unwilling to detect and identify abusive users who send bullying and harassing messages. These apps are also unable or unwilling to enforce their policies where they state they would ban, reveal, and report abusive users. Compl. ¶ 181.

Other examples of relevant allegations in the Original Complaint and the FAC include, but are not limited to, the following:

A. In the Original Complaint:

i. "YOLO stated that it would reveal the identifies and ban users who engage in bullying and harassing behavior. YOLO stated that it has a zero-tolerance policy for bullying." Compl. ¶ 2 (emphasis in original).

ii. "To prevent harm, the apps must enforce their own rule that deters abusive users by reporting to authorities and parents, revealing their identities and banning them from the apps." Compl. ¶ 16.

iii. "Upon information and belief, Carson relied on YOLO's misrepresentation that YOLO would reveal the identifies of the aggressors." Compl. ¶ 21.

iv. "On the first screen of the user's interface with the app, YOLO states, "No bullying. If you send harassing messages to our users, your identity will be revealed." Compl. ¶ 23.

v. "In the most visible places, YOLO falsely represented it would take concrete actions to enforce safeguards: that the abusive users' accounts will be banned and their identities will be revealed." Compl. ¶ 24.

vi. "If YOLO had followed its own stated policy and revealed the identities or banned abusive users, more users would be deterred from engaging in harassing or bullying because they would know they would be held accountable for their actions." Compl. ¶ 26.

vii. "Contrary to the representation that YOLO would ban and reveal users who are engaging in bullying and harassment, YOLO failed to identify, detect, prevent, protect, or otherwise take any action to prevent the harm that Carson suffered using the YOLO app. YOLO's misrepresentations were material and resulted in the injury suffered by Carson and other consumers." Compl. ¶ 27 (emphasis in original).

viii. "As a direct result of the defective and unreasonably dangerous design of the Defendants' apps, Plaintiff Carson Bride suffered from bullying and harassment by unknown users on Defendants' apps and suffered while being unsuccessful at getting Defendants' apps to reveal the identities of those sending harassing messages." Compl. ¶ 46.

ix. "Defendants made false statements about enforcing a zero-tolerance policy against bullying and harassing behavior, including banning users and revealing their identity, reporting harassment by users, and removing third-party apps that lack adequate safeguards against bullying and harassing behavior." Compl. ¶ 53.

B. In the FAC:

i. "[I] in the most visible places when users signed up for YOLO, Yolo falsely represented that its app would take concrete actions to implement safety measures—namely that abusive users' identities would be revealed and their accounts would be banned—and that there would be 'no tolerance for objectionable content or abusive users.'" FAC at 27.

ii. "Yolo and Lightspace failed to provide adequate warnings about the dangers associated with the use of anonymous messaging, and about how the purported safeguards against such dangers (such as monitoring, reporting, banning, and revealing identities of users) are not effective to stop bullying and harassment on anonymous messaging apps. Instead Yolo and Lightspace falsely represented the safety of their products and falsely described YOLO and LMK's alleged intolerance for objectionable conduct by users." FAC at 62.

iii. "[W]hen YOLO's users were signing up for YOLO, Yolo made material representations

that it would take concrete actions to implement safety measures, namely that abusive users' identities would be revealed and their accounts would be banned, and that there would be 'no tolerance for objectionable content or abusive users.'" FAC at 65.

iv. "From the earliest days that YOLO was operational through the time that YOLO was banned by Snap in 2021, YOLO routinely did not reveal the identifies of abusive users, nor did YOLO ban those users, even after abusive users were reported to Yolo." FAC at 65.

v. "And when Yolo made these statements, it knew that it did not have a system in place or the resources to regularly perform the actions that Yolo stated it would undertake, such as revealing and banning users who bullied or harassed other users." FAC at 66-67.

Appellee's claim that the FAC only described "reveal and ban" feature as a pop-up message or notice to users is a woeful and bad-faith mischaracterization of the FAC's actual description of the feature: a purported safeguard that was ultimately not effective.

According to Appellee's motion to strike, the reveal and ban feature was argued as a basis for the misrepresentation claim instead of the product liability claims. However, both the Original Complaint and FAC often reference the YOLO app's lack of capability to enforce the policy to reveal and ban bad actors. For instance, example (viii) from the Original Complaint and example (ii) from the FAC refer to this reveal and

ban feature as part of YOLO's "defective and unreasonably dangerous design" and "purported safeguards."

2. One-Way, Targeted Messaging Was Already Pleaded and Fully Described in the Pleadings

Appellee assert one-way messaging was not mentioned in the FAC. Appellee's argument is only a semantic one: the descriptions of this one-way anonymity feature were emphasized throughout both the Original Complaint and the FAC. Specifically, the descriptions of how YOLO works contain numerous mentions of how anonymity attaches to the "senders" of the YOLO messages, while recipients have no control over how to reveal the senders. The non-exhaustive list below includes examples from excerpts of the Original Complaint and FAC:

1. "[T]he apps allow teens to chat, exchange questions and answers, and sending polling requests to one another on a completely anonymous basis—that is, the receiver of a message will not know the sender's account names, nicknames, online IDs, phone numbers, nor any other identifying information unless the sender "reveals" himself or herself by "swiping up" in the app." Compl. at 14; FAC at 12 (emphasis added).

2. "In responding to numerous abusive messages, Carson asked the anonymous users sending him abusive messages to voluntarily "S/U" (Swipe Up) to reveal their identities. None of the users chose to reveal themselves." Compl. at 21; FAC at 35 (emphasis added).

3. "YOLO's anonymous app hinders parents, guardians, and educators from taking action because they do not know who the sender of the message might be." Compl. at 28 (emphasis added).

4. "[W]e are requesting the contacts of every Snapchat/YOLO anonymous user who sent a message to my son's Snapchat account during the month of June 2020." Compl. at 28 (quoting Carson's parents' email to Yolo Technologies, Inc.) (cleaned up).

The fact one of the central features at issue in this matter involves "revealing" anonymous users already establishes the one-way messaging feature. As repeatedly alleged in the pleadings, in the days leading up to Carson's death, he repeatedly searched for ways to reveal his bullies' and harassers' usernames on the YOLO website and third-party search engines. Compl. at 20, 21-22; FAC at 5. The pleadings made clear allegations that Carson's bullies and harassers were able to identify him and direct abusive messages to him when they sent the messages. In contrast, Carson desperately tried to uncover the identities of the users sending him abusive messages and was ultimately unsuccessful. Is this reality alone not enough for Appellee to recognize that one-way messaging has been a key feature of this matter from the start?

While it is well established that the Ninth Circuit does not consider new issues or claims raised for the first time in a reply brief, the issues that Appellee seeks to strike were identified and briefed from the beginning of this litigation. Hence, Appellee cannot establish strikable reasons such as: (1) failure to include a claim in an initial pretrial order, as in *Eberle*

v. City of Anaheim, 901 F.2d 814, 817-18 (9th Cir. 1990); (2) failure to raise a standing issue in an opening brief, as in *Hillis Motors, Inc. v. Hawaii Auto. Dealers' Ass'n*, 997 F.2d 581, 584 n. 4 (9th Cir. 1993); and (3) failure to challenge a lower court's conclusion of law, *Committee v. Yost*, 92 F.3d 814, 819 n. 3 (9th Cir. 1996).

Here, Plaintiffs-Appellants connected the YOLO app's advertised features—anonymous messaging, one-way messaging, and reveal and ban function—to the product liability claim raised in both the Original Complaint and FAC. Misrepresentations about the YOLO app contribute to the product's inherently dangerous quality because Appellee's inability to deliver on its promise of safety is connected to the app's advertised features. These features were discussed at length prior to the Reply Brief. Connecting these discussions to a claim raised in initial pretrial orders cannot be said to have risen to the level of introducing new claims or issues for the first time in a reply brief.

CONCLUSION

For the aforementioned reasons, Defendant-Appellee's motion to strike should be denied in its entirety.

EISENBERG & BAUM, LLP

By: /s/ Juyoun Han
Juyoun Han, Esq.
Attorneys for Plaintiffs-Appellants

DATED: March 8, 2024

REPLY BRIEF FOR PLAINTIFFS-APPELLANTS (JANUARY 12, 2024)

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

THE ESTATE OF CARSON BRIDE, by and through his appointed administrator KRISTIN BRIDE; A.K., by and through her legal guardian JANE DOE 1; A.C., by and through her legal guardian JANE DOE 2; A.O., by and through her legal guardian JANE DOE 3; TYLER CLEMENTI FOUNDATION, on behalf of themselves and all others similarly situated,

Plaintiffs-Appellants,

v.

YOLO TECHNOLOGIES, INC.,

Defendant-Appellee.

No. 23-55134

On Appeal from the United States District Court for the Central District of California

Juyoun Han
Patrick K. Lin
Eric Baum
EISENBERG & BAUM, LLP
24 Union Square East, Penthouse
New York, New York 10003
Telephone: (212) 353-8700

Attorneys for Plaintiffs-Appellants

{ Internal Table of Contents
and Table of Authorities Omitted }

INTRODUCTION

This lawsuit was brought by Plaintiffs-Appellants (hereinafter, the "Children") who were harmed, some fatally, by dangerous mobile applications marketed to children with false promises of safety. In the current market, digital technology products often incentivize danger to maximize profit: Danger brings audience, audience brings data, and data brings profit. From posts and broadcasts daring teenagers to race to find a pop-up celebrity, to speed filters on Snapchat App encouraging teenagers to drive at fatally dangerous speeds, product developers have knowingly exploited the vulnerable psychology of naïve teenagers to seek thrills, dopamine, and adrenaline by incorporating and romanticizing danger and risk in their products. This Court in *Lemmon* held that product developers who monetize such dangers would face accountability under the law, and that they could not seek cover under the CDA.

YOLO made design choices in its anonymous messaging app that would heighten the danger and amplify users' engagement. Essentially every anony-

mous messaging app had been known to be dangerous, risky, daring, and thus, to attract an instant pool of audience among young users, guaranteeing a short term success to companies that develop them. For more than a decade, anonymous apps have also come to be associated with teen suicide for the same reasons. An exhaustive list of previous anonymous messaging apps that hit the top of the app markets are provided in the Children's Complaint, along with names of children who took their lives due to the harms engendered by those apps.

YOLO's advertised features were uniquely dangerous: it allowed for one-way anonymous messaging, which meant that only the sender of the message would be anonymous. Meanwhile, if the non-anonymous recipient of the message wished to reply to the anonymous message sender, it needed to do so in a semi-public forum, where it had to disclose the anonymously-received message to all of their connected audience because the recipient would not know the specific person to reply to. YOLO's design choice engages not only the receiver and sender but involves connected audiences in the conversation. It is by no coincidence that such design would boost user engagement, increasing profit for the platforms. In the meantime, it became the breeding ground for anonymous cyber-bullies to intentionally target their victims, who were not anonymous, and publicly humiliate them before a large audience. YOLO also designed two "reveal" functions: first the anonymous sender can unilaterally elect to "swipe to reveal" their own identity; and second, YOLO voluntarily represented that it would "reveal" the identities of users who harass or bully other users or "ban" such users. Problematically, this

latter "reveal" function did not work — all of the Children remembered seeing this purported "reveal" function by YOLO but were ignored when they attempted to use the function to reveal the identities of their vicious harassers. YOLO's false promise of the "reveal" and "ban" function was different from other types of community policy guidelines because it was conspicuously advertised as part of its platform's feature. The Children were misled by this promise and the Plaintiff-Appellant Carson Bride spent the last frantic minutes of his life desperately trying to find out how to reveal the identities of bullies on YOLO.

Ignoring all of these specific details about YOLO's design, the District Court erred by analogizing YOLO to the pseudonymous community board in *Dyroff* where all users' identities are associated with a pseudonym, and cursorily concluded that YOLO's reveal and ban feature is merely a content moderation decision which should be protected under CDA. But YOLO did not have to advertise and misrepresent the reveal and ban, nor did it have to make its designs so conducive to bullying without any recourse for the bullying victim. YOLO intentionally designed its product to maximize recklessness, danger, engagement, and ultimately profit, and now seeks to hide under an irrational interpretation of the CDA.

Since 1996, in the near three decades that the Communication Decency Act has been in effect, digital technology tools have become smart, sophisticated, and covertly invasive. Hence, Courts are now more skeptical about digital communication platforms who play down their roles to passive publishers. "As the internet has exploded, internet service providers have moved from 'passive facilitators to active operators.'

They monitor and monetize content, while simultaneously promising to protect young and vulnerable users." *Doe v. Snap, Inc.*, No. 22-20543, at *7 (5th Cir. Jun. 26, 2023) (Elrod, J., dissenting from denial of rehearing en banc).

Technology may appear simple through an interface, but the devil is in the details of its designs: product teams use various features and tools, often hidden or behind-the-scenes, to increase engagement, promote content, and raise revenue. For example, different ride-sharing apps employ designs that boost the collection of tips or to gain more customers. Video and music streaming platforms compete with algorithms and designs to recommend contents that continue to keep users engaged. Similarly, social media and messaging apps utilize features such as daily streaks, push notifications, and other tools meticulously designed to boost user engagement. The point of these features is not about brokering rides or publishing content — it is about boosting business operations by increasing user engagement, which means more data, and more profit.

In recent decisions such as the Social Media Cases in the California Supreme Court, the court sharply pointed out that platforms are not immune from liability under the CDA simply because a particular claim involves content. Rather, the court held that the CDA does not cut off liability for business conduct related to how their platforms were designed, independent of the content published on those platforms. *See In re Coordinated Proceeding Special Title Rule 3.550 Soc. Media Cases*, 2023 Cal. Super. LEXIS 76992 (Los Angeles Cty. Sup. Ct. Oct. 13, 2023). Similarly, the Seventh Circuit court recently decided

that platforms cannot benefit from CDA protection if the claims arise from publication of illegal content, but can held accountable as product developers for designing, supporting, marketing, operating, and facilitating a product. *G. G. v. Salesforce.com, Inc.*, No. 22-2621 (7th Cir. Aug. 3, 2023).

ARGUMENTS

This Court in *Barnes v. Yahoo!, Inc.* established its seminal three-pronged test for determining whether an internet company may be exempt from liability under Section 230. 570 F.3d 1096, 1100 (9th Cir. 2009). Under this test, immunity from liability exists for "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider." *Id.* at 1100-01. On appeal, the Children assert that the District Court erroneously applied the second and third prong of the Barnes test, and that this Court should reverse the lower court's decision to dismiss the action.

A. Section 230 Does Not Offer Protection to YOLO Because Children Seek to Hold YOLO Accountable for Its Own Conduct, Not Its Content

With respect to both the second and third prongs of the *Barnes* test, the disputed issue here is whether the Appellants claimed that YOLO is liable for its own content or for third-party users' content. *See* 570 F.3d 1096, 1100 (9th Cir. 2009). The District Court's decision contained erroneous rulings in two distinct aspects: duty and causation. In this appeal, this Court must

determine whether the claims alleged by Children derive from YOLO's duty as a publisher or duty as a developer, operator, creator and advertiser of its own product. As stated in the Opening Brief, Children have sufficiently alleged that its claims against YOLO were not about its publication of third party users' content but about YOLO's own conduct and content.

As to causation, this Court must review whether the Children have plausibly alleged that YOLO's non-publishing conduct caused the stated harms. This requires a fact-specific inquiry regarding the alleged conduct (*i.e.*, the development of the application) and the harms upon the Children (*i.e.*, the inability to face the harassers, constant targeting in a one-way anonymity, impossibility of guardians to be involved, hopelessness and fear about unknown harassers, abandoned trust and harm from misrepresentation that harassers would be revealed or banned, generating motivation to target more harassment, etc).

B. The Children's Claims Focus on YOLO's Failure of Duty as Developers of Its Own Product and Content, And CDA Does Not Bar Such Claims

The CDA bars claims only when it holds a platform liable as a publisher of third party content. This concept of CDA protection has metastasized beyond its intent mainly because courts had difficulty interpreting the concept of publisher treatment. To properly understand whether liability hinges on a publisher duty, the Court must first examine the duty underlying the claims. YOLO superficially argues that the "option to anonymize email addresses" and setting forth an anonymous posting board are by nature

related to publishing content and thus entitled to CDA protection. YOLO Br. at 24 *(citing Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116, 1124 (N.D. Cal. 2016); *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1098 (9th Cir. 2019)). However, this Court and others have held that performing a publishing function does not necessarily mean that the platform is acting out of a publisher duty. The publisher duty analysis must reach beyond actions and ask where that duty comes from. Assuming arguendo that anonymizing user information is a publisher function, if that function was performed to fulfill a contractual promise or a commercial representation, the duty to anonymize user information derives from the contract or the representation, not by virtue of being a traditional publisher.

This Court has already recognized the importance of analyzing a platform's duty to remove content when it did so for each claim in *Barnes,* differentiating between a publisher's duty and a non-publisher's duty with respect to Section 230. In *Barnes*, while this Court found that Section 230 immunized Yahoo from the plaintiff's negligence claims because the duty arose from Yahoo's role as a publisher, it held Yahoo liable on the plaintiff's promissory estoppel claim because that duty arose from Yahoo's contractual obligation to remove particular injurious content. *Barnes*, 570 F.3d at 1107 ("Barnes does not seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promisor who has breached."). This Court explained that "[c]ontract 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." *Id.* at 1107.

YOLO seeks to distinguish *Barnes* from this case by stating that *Barnes* involved a promissory estoppel/breach-of-promise claim for which this Court found no CDA immunity, and that the instant case does not bring contractual claims. YOLO Br. at 27. YOLO misses the mark of *Barnes*, because the significance of this Court's *Barnes* decision is that a different duty analysis can attach to the platform's removal of conduct — a publisher duty and a non-publisher duty (*i.e.*, a contract or promissory estoppel claim). *Barnes*, 570 F.3d at 1107. And applied here, *Barnes* would support that the CDA would not bar the Children's negligence, misrepresentation, and duty to warn claims.

Following the wisdom of this Court in *Barnes*, courts around the country are now more informed and aware that a traditional publisher role does not cover the actions and decisions involved in designing, developing, operating, and distributing social media products.[1] These courts have been able to parse out the duties of social media product developers that correspond with non-publisher roles as to their products.

For example, in a recent decision by the Seventh Circuit in *G. G. v. Salesforce.com, Inc.*, the Court

---

[1] Large, modern-day internet platforms are more than willing to remove, suppress, flag, amplify, promote and otherwise curate the content on their sites in order to cultivate specific messages." *See Missouri v. Biden*, 83 F.4th 350, 392 (5th Cir. 2023), cert. granted, No. 23-411, 2023 WL 6935337 (S. Ct. Oct. 20, 2023) (finding numerous platforms likely restricted protected speech on their sites as a result of government pressure).

reiterated the distinction between a platform's conduct and publication through a well-articulated duty analysis. 76 F.4th 544 (7th Cir. 2023). It rejected the defendant's invocation of Section 230 to dismiss the case because the plaintiffs sought to hold Salesforce accountable for its actions, not for what it published. In *Salesforce.com*, a minor-plaintiff and her mother brought suit under the Trafficking Victims Protection Reauthorization Act of 2003 (Section 1595). *Id.* at 548. A sex trafficker used the now defunct Backpage.com to advertise G.G. while Salesforce helped Backpage reach more customers. This Court found that Salesforce was not entitled to dismissal under Section 230 because the plaintiffs sought to hold Salesforce "liable under Section 1595 for its own . . . acts or practices, rather than for publishing content created by another." *Salesforce.com*, 76 F.4th at 567 (emphasis added):

> [P]laintiffs seek to hold Salesforce accountable for supporting Backpage, for expanding Backpage's business, for providing Backpage with technology, for designing custom software for Backpage, for facilitating the trafficking of G.G., for helping Backpage with managing its customer relationships, streamlining its business practices, and improving its profitability, and for enabling Backpage to scale its operations and increase the trafficking conducted on Backpage.

Id. (internal quotations omitted). The plaintiffs alleged that Salesforce had a duty not to benefit knowingly from participating in Backpage's venture while knowing or having reason to know that the venture was engaged in sex trafficking. *Id.* The Seventh Circuit Court found "[t]hat duty does not depend in any way

on Salesforce's supposed status or conduct as a publisher or speaker." *Id.* (internal quotations omitted); *see also Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1101-02 (9th Cir. 2009). If the duty originates from the platform's own conduct or business practices—such as developing, designing, and operating a commercial product or making representations upon which consumers rely upon—rather than for publishing content created by another, then the second prong is not met and Section 230 does not apply. Salesforce.com, 76 F.4th at 567.

In another recent decision in the *Social Media Cases* in the California Supreme Court, the plaintiffs alleged various social media companies design platforms with manipulative and addictive features. *See In re Coordinated Proceeding Special Title Rule 3.550 Soc. Media Cases* ("Social Media Cases"), 2023 Cal. Super. LEXIS 76992. In denying the defendants' motion to dismiss, Judge Kuhl in the *Social Media Cases* correctly conducted a duty analysis, poignantly reasoning that "not all legal duties owed by Internet intermediaries necessarily treat them as the publishers of third party content, even when these obligations are in some way associated with their publication of this material." *Social Media Cases*, 2023 Cal. Super. LEXIS 76992, at *30. The Judge continued, "[it may very well be that a jury would find that Plaintiffs were addicted to Defendants' platforms because of the third-party content posted thereon. But the Master Complaint nonetheless can be read to state the contrary—that is, that it was the design of Defendants' platforms themselves that caused minor users to become addicted." *Id.* at *29-30.

Judge Kuhl drew a critical distinction that Section 230 does not apply when plaintiffs attempt to

hold platforms, namely social media companies, liable for the ways in which they "designed and operated their platforms," not the content on the platforms. *Id.* at *2. As the Ninth Circuit found in *Lemmon v. Snap, Inc.*:

> Snap is an internet publishing business. Without publishing user content, it would not exist. But though publishing content is a but-for cause of just about everything Snap is involved in, that does not mean that the [plaintiffs'] claim, specifically, seeks to hold Snap responsible in its capacity as a publisher or speaker. The duty to design a reasonably safe product is fully independent of Snap's role in monitoring or publishing third-party content.

955 F.3d 1085, 1092-93 (9th Cir. 2021) (internal quotations omitted). Judge Kuhl warns that courts should be cautious "not to stretch the immunity provision of Section 230 beyond its plain meaning in a manner that diminishes users' control over content they receive." *Social Media Cases*, 2023 Cal. Super. LEXIS 76992, at *100. "So long as providers are not punished for publishing third-party content, it is consistent with the purposes of Section 230 to recognize a common law duty that providers refrain from actions that injure minor users." *Id.* at 100-01.

Just like the Seventh Circuit Court in *Salesforce* determined that the CDA does not shield claims against business conduct and product design (*e.g.*, supporting, expanding, designing, facilitating, and improving profitability of a website where it knew or had reason to know sex trafficking was occurring), and Judge Kuhl in the *Social Media Cases* found it

plausible that the design of a platform can be addictive, independent of the contents published therein, the District Court here should have found that YOLO may be sued for its own conduct or business practices—such as developing, designing, and operating a commercial product or making representations upon which consumers rely upon.

The Amended Complaint plausibly alleged that the claims were predicated upon product developer duties, not a publisher duty:

> One of the duties that Yolo [] violated springs from the duty to take reasonable measures to design a product that is more useful than it was foreseeably dangerous. By simply removing the element of anonymity, Yolo []could have complied with this duty to design a reasonably safe product. It could have provided the same messaging tools—such as the ability of users to send polling requests to each other—without monitoring or changing the content of the messages. Likewise, Yolo [] could have complied with their duty to warn users (and users' parents and guardians) of the danger of anonymous messaging without monitoring or changing the content of users' messages. And Yolo [] could have complied with their duties under the common law and state statutory law not to make false, deceptive, or misleading statements simply by accurately describing their own products, services, and business practices, or by ¶not making such statements at all. ER-23-24 (AC ¶ 18).

Further, the Amended Complaint pointed out that it was not the content, but YOLO's enabling of one-way anonymous messages as well as the false promise to ban or reveal harassing users, that produced harms independent of the content itself:

> Carson's continued and painstaking efforts to investigate his harassers' identity until moments before his death demonstrates the tormenting anxiety and pressure that YOLO's anonymity feature imposed on him. See ER-52 (AC ¶ 97).
>
> Anonymity hinders victims from appropriately handling the content of messages because it deprives them of any means of confronting the perpetrators or assessing the possible reasons for those messages, and this leaves a sense of unresolved anger and harm especially in developing teenagers that makes it impossible for guardians, schools, or law enforcement to intervene. See ER-39 (AC ¶ 56).
>
> Moreover, YOLO's false statement creates a new type of harm that is separate from the third-party messages. This includes the level of stress and frustration that was experienced by Carson as he was searching online for means to reveal his YOLO bullies on the night prior to his death. See ER-51 (AC ¶ 94). Similarly, A.K., A.O., and A.C. were harmed when they all relied upon YOLO's statement that harassing users will be unmasked, and later their requests to reveal the identities of harassers were ignored. *See* ER-57-60 (AC ¶¶ 122-48).

The development of anonymous apps like YOLO's was not just about publishing content. YOLO made a calculated decision to design an anonymous messaging app that allow for one-way targeting of messages under a false promise to reveal or ban bad actors. Here, the Children's Complaint centers on YOLO's duty as product developers, not as publishers.

C. A Simple "But-For" Test, Used By The District Court, Is Inadequate for Determining Whether the CDA Shield Applies

The District Court's decision collapsed the analysis of duty and causation question by relying on a "but-for" test, reasoning in its decision, "had those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable." ER-12. YOLO implicitly concedes that the "but-for" test would be an inadequate analysis by arguing that "the Putative Class Members' attempt to recast the District Court's sound analysis as using a 'but-for' third party content publication test is without merit." YOLO Br. at 28.

In the *Social Media Cases*, Judge Kuhl ruled that "courts have repeatedly 'rejected use of a but-for test that would provide immunity under [Section 230] solely because of a cause of action would not otherwise have accrued but for the third-party content." *Social Media Cases*, 2023 Cal. Super. LEXIS 76992, at *103 (citing *Lee v. Amazon.com, Inc.*, 76 Cal. App. 5th 200, 256 (2022)) (internal citations and quotations omitted). In *Doe v. Internet Brands, Inc.*, this Court ruled that a "but-for" test would "stretch the CDA beyond its narrow language and its purpose." 824 F.3d 846, 853

(9th Cir. 2016). *See, e.g., HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 682 (9th Cir. 2019) *("Internet Brands* rejected use of a but-for test that would provide immunity under the CDA solely because a cause of action would not otherwise have accrued but for the third-party content.").

YOLO contends that it was a publisher for purposes of this lawsuit. However, the fact that publishing was involved somewhere in the harassment and bullying that young Carson Bride was subjected to does not mean that YOLO can successfully use Section 230(c) to shield itself from liability. *Salesforce.com*, 76 F.4th at 567. Publishing activity was "a but-for cause of just about everything" YOLO was involved in. *See Doe v. Internet Brands, Inc.*, 824 F.3d 846, 853 (9th Cir. 2016). The obtuseness of the "but-for" test should be replaced with a concrete duty analysis as outline in the previous section.

D. CDA Does Not Apply Per *Barnes* Third Prong Because YOLO's Own Content Caused the Harm and Its Designs Materially Contributed to Dangerous and Harmful Content

Two important points are reiterated regarding *Barnes* third prong: The Children's claims are focused on YOLO's own content, not that of any other user; and the Complaint alleged that YOLO's own designs materially contributed to the danger and harm alleged in the claims. The disputed issue here is whether the Children claimed that YOLO should be liable for its own content or for content provided by another information content provider. *See* Barnes, 570 F.3d at 1100. Here, the District Court first erred by not distinguishing the failure to warn and misrepresenta-

tion claims which solely focus on YOLO's own statements and conduct: a conspicuous and misleading notification that it would reveal and ban bad actors on the platform. Secondly, the District Court failed to engage with the facts specific to this case, which are distinguishable from *Dyroff* YOLO leads this Court to assume without basis that "YOLO app's anonymity feature [] is a neutral tool that the user exploits in creating harmful content." YOLO Br. at 32 (citing *Dyroff*, 934 F.3d at 1098).

First, as sufficiently explained in the Children's Opening Brief (Appellants' Opening Br. at 32-40), the CDA does not bar claims that are based on the platform's own internet content, or where the claims are predicated on the platform's own acts. *See Lemmon*, 995 F. 2d at 1093. Children's Failure to Warn Claims and Misrepresentation and False Advertising claims are solely predicated on YOLO's own content and conduct of misstating and misrepresenting its product. And the Children's Complaint cogently alleges that YOLO's own statements resolving to reveal and ban harassing users created an expectation and reliance in the Children's mind which then turned into disappointment and stress when the platform failed to carry out its promise. Children Opening Br. at 12 (citing ER-51 & 57-60). The Complaint alleged that Carson's last search online was to reveal users on YOLO, and it is plausible that the frustration of not being able to reach YOLO to do so may have very well been the last straw that led to his death. *Id.* The Children should have had the opportunity to discover and present these facts to a jury.

Second, the Complaint sufficiently stated that YOLO's own conduct—its deliberate product design

choices—materially encouraged the dangers on its platform and should not have been barred. Children's Opening Br. at 38 (citing ER-18-19; ER-44-45; ER-52. "Immunity from design defect claims is neither textually supported nor logical because such claims fundamentally revolve around the platforms' conduct, not third-party conduct. Nowhere in its text does Section 230 provide immunity for the platforms' own conduct." *Snap*, No. 22-20543, at *5 (Elrod, dissenting). "Product liability claims do not treat platforms as speakers or publishers of content." *Id.*

Under the material contribution test, a platform materially contributes content if the features are conducive to a particular type of content that is harmful. In that case, the platform cannot claim Section 230 protection. The Ninth Circuit has held that a website that "creat[es] or develop[s]" content "by making a material contribution to [its] creation or development" loses Section 230 immunity. *Gonzalez v. Google LLC*, 2. F.4th 871, 892 (9th Cir. 2021) (citing *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1269 (9th Cir. 2016)). A "material contribution" does not refer to "merely . . . augmenting the content generally, but to materially contributing to its alleged unlawfulness." *Fair Hous. Council of San Fernando Valley v. Roommates, com*, 521 F.3d 1157, 1167-68 (9th Cir. 2008). This test "draw[s] the line at the crucial distinction between, on the one hand, taking actions" to display "actionable content and, on the other hand, responsibility for what makes the displayed content [itself] illegal or actionable." *Kimzey*, 836 F.3d at 1269 n.4 (internal quotations omitted) (quoting *Jones v. Dirty World Ent. Recordings LLC*, 755 F.3d 398, 413-14 (6th Cir. 2014)).

The District Court and YOLO seek to analogize the facts of this case to *Dyroff,* but the superficial similarities do not account for the differences in the designs of the pseudonymous posting board in *Dyroff* where everyone's registration credentials were attached to their messages and afforded multilateral pseudonymous communication to all users.

In contrast, YOLO's advertised features were anonymous, one-way messaging and a purported function to reveal and ban bad actors. While YOLO succeeded in delivering its one-way, anonymous messaging feature, its reveal-and-ban function was either a failure or a lie. This perfect storm resulted in a product that is harmful no matter what the content might be. Appellee-Defendant claims its anonymity feature is content-neutral; however, this is a disingenuous claim that does not account for the complete picture of YOLO as a product. YOLO's anonymity feature and one-way communication and failure to reveal and ban bad actors breeds harm regardless of the content or the platform. These three features must be taken together as part of a material contribution analysis. As described in Plaintiffs-Appellants' Opening Brief, it is the combination of these features that make YOLO an inherently dangerous product. *See* ER-24 ("YOLO created a virtual invisibility cloak with a falsely advertised safety switch that did not work, and reaped millions of downloads of its app—countless of those downloads were by vulnerable young users who suffered harm."; "YOLO's false statement creates a new type of harm that is separate from the third-party messages.").

While YOLO's anonymous, one-way messaging feature allowed other users to incessantly terrorize

Carson and other Plaintiffs-Appellants, it is YOLO's defective reveal-and-ban feature that hindered users' control over their product experience, enabled bullies to avoid consequences, and ultimately keep both harassers and victims engaged with the platform as victims desperately try to uncover the identity of their bullies. Failing to deliver on its advertised reveal-and-ban feature meant YOLO not only facilitated the severity and frequency of bullying online but ensured victims could not report the bully to their parents, school officials, or trusted adults offline.

Here, the Complaint sufficiently alleged that the specific harm—the targeted bullying and harassment—is attributable to YOLO's anonymity feature. It is true Section 230 prevents platforms like YOLO from being held accountable for the content third-party users send to users, even if that content is hateful and harmful. However, the harmful content, frequency of transmission, and the inability of victims to seek recourse are all the result of YOLO's design, not its content or moderation policies. Anonymity emboldens users to harass without fear of consequence, which not only enables the initial harassment but incentivizes repeated and often increasingly hostile instances of harassment. The anonymity design baked into YOLO's platform also inhibits users from having more agency over their experience on the platform because they cannot respond to the harmful or harassing communications unless they publicly reveal the messages in a humiliating fashion.

Section 230(c) may be relevant to liability for claims that depend on who "publishes" information or is a "speaker"—for example, in cases involving defamation, obscenity, or copyright infringement—but

where the claim does not depend on publishing or speaking, Section 230(c) is irrelevant. *Salesforce.com*, 76 F.4th at 565 (internal citations omitted). There are instances where Section 230 is a valuable and even essential mechanism for facilitating freedom of expression on online platforms. When comments are made on an Instagram post or YouTube video or when replies are added to a Reddit thread or Facebook post, Section 230 protects those platforms. In those instances, users are publicly expressing themselves to other users in two-way digital spaces, meaning other users can react, share, agree, disagree, and everything else in between. Here, YOLO's core anonymity feature allows users to privately speak at other users in a one-way digital space. In other words, bullies can seek out and target victims, relentlessly terrorizing them with hateful and harmful messages. Meanwhile, the victim is left desperately trying to learn the identity of their bully. If the same bully contacted a victim on Instagram, Facebook, or many other platforms, and sent the same content, the victim can identify the bully, respond to them, and block their communications. As such, the content of these communications are not the primary issue at hand, rather it is the design decision to allow bullies to use a shield of anonymity to harass others without recourse.

Appellee-Defendant argues that all the harms are caused by the messages and not the designs. But this is an issue of causation, not duty, and deserves to be explored in discovery. Just as Judge Kuhl recognized that a jury may attribute harms to the third-party content on platforms *or* the design of the platforms themselves, *Social Media Cases*, No. JCCP 5255 at *100, a jury in this case may do the same.

Accordingly, a fact-specific inquiry is necessary when applying the material contribution test. To that end, Plaintiffs-Appellants request this Court to allow this case to go into discovery so that a jury might judge the cause of these harms for themselves.

CONCLUSION

For the reasons argued above, this Court should find that the District Court erroneously applied the second and third prong of the *Barnes* test, and reverse the lower court's decision to dismiss the action.

Respectfully submitted,

By: /s/ Juyoun Han
Eric M. Baum
Eisenberg & Baum LLP
24 Union Square East, Penthouse
New York, NY 10003
(212) 353-8700

Attorneys for Plaintiffs-Appellants

Dated: January 12, 2024