**No. 23-55134**

---

**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.,

*Defendant-Appellee*.

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

---

# YOLO TECHNOLOGIES, INC.'S ANSWERING BRIEF

---

Nick S. Pujji (SBN 259571)
Carol Yur (SBN 290145)
Emma Moralyan (SBN 311511)
Dentons US LLP
601 S. Figueroa St., Suite 2500
Los Angeles, CA 90017
Tel.: 213-623-9300

Attorneys for Appellee YOLO Technologies, Inc.

## CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1(a), YOLO Technologies, Inc. states that it does not have a parent corporation and no publicly held corporation owns 10% or more of YOLO Technologies, Inc.'s stock.

Dated: November 22, 2023

DENTONS US LLP

*/s/ Nick S. Pujji*
Nick S. Pujji
Carol Yur
Emma Moralyan

*Attorneys for Appellee YOLO Technologies, Inc.*

## TABLE OF CONTENTS

**Page**

## TABLE OF AUTHORITIES

**Page(s)**

**Cases**

## Statutes



## Other Authorities

## INTRODUCTION

The issues presented by this appeal are straightforward: the District Court correctly applied settled law in holding Appellants the Estate of Carson Bride, the Tyler Clementi Foundation, A.K., A.C., and A.O.'s (the "Appellants" or "Putative Class Members") claims were barred by the broad statutory immunity afforded to interactive computer service providers under the Communications Decency Act of 1996 ("CDA"), 47 U.S.C. § 230 ("Section 230"). Because the Putative Class Members cannot demonstrate any error in that ruling, this Court should affirm the judgment of dismissal for Defendant-Appellee YOLO Technologies, Inc. ("YOLO").

In so doing, the Court will protect a foundational pillar that supports the growth and preservation of a key national interest – the Internet. Section 230 of the CDA grants immunity to Internet publishers of content created or developed *not by them*, but instead by third parties. Congress enacted this law to promote the free exchange of information and ideas over the Internet, and to encourage voluntary monitoring for offensive or obscene material. Recognizing this important national interest, Congress expressly noted in the law itself that "[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation," and that "[i]ncreasingly Americans are relying on interactive media for a variety of political, educational, cultural, and

entertainment services." 47 U.S.C. § 230(a)(4), (5). Furthermore, Congress declared it the "policy of the United States" to "promote the continued development of the Internet and other interactive computer services" and "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[.]" 47 U.S.C. § 230(b)(1), (2).

Here, the Putative Class Members sued YOLO claiming they (or in the Foundation's case, its members) allegedly suffered harm as a result of the anonymous messages received through the online app (the "YOLO app") developed by YOLO. The District Court correctly held the Putative Class Members' efforts to plead around Section 230 were ineffective because their product liability, misrepresentation, and associated state-law claims were all premised on activities that fall within the scope of the Section 230's immunity, *e.g.*, publishing third-party user content and content moderation. As the District Court recognized, if creatively reframing immunized conduct in the guise of state-law tort claims could defeat immunity, then Section 230 and the important public policies Congress enacted it to promote would become empty letters.

At bottom, the Putative Class Members are simply asking this Court to rewrite the CDA, and its established precedent, to create liability that does not otherwise

exist. YOLO respectfully requests this Court deny the Putative Class Members' request in its entirety, and affirm the order of dismissal.

## JURISDICTIONAL STATEMENT

YOLO agrees with the Putative Class Members' statement as demonstrating the jurisdiction of the District Court and of this Court.

## STATEMENT OF THE CASE[1]

### 1. The YOLO app Allowed Users to Send Messages to Each Other on a Completely Anonymous Basis

YOLO is an online application ("app") developer. In 2019, it launched the YOLO app – an anonymous messaging app that was made available to the public as an extension to Snapchat. (ER18–19, ER-27–28). Within a week of the YOLO app's launch, it became the top downloaded app in America and a "teen hit"; within months, the app had 10 million active users. (ER-19).

The YOLO app was "an app designed to allow its users to send messages to each other anonymously," and was predominantly used by teens. (ER-27–28). The YOLO app "allows teens to chat, exchange questions and answers, and send polling requests to one another on a completely anonymous basis."[2] (ER-27–28). The

[1] Because this appeal addresses the District Court's order granting YOLO's Motion to Dismiss the First Amended Complaint ("FAC"), the statement of the case is drawn exclusively from the FAC and the evidence the parties offered below in connection with YOLO's Motion to Dismiss. YOLO admits none of the Putative Class Members' claims, theories, or allegations.

[2] As further explained in this brief, the FAC fails to allege any facts to support the claim the YOLO app is a "one-sided, anonymous messaging app" that required

receiver of a message will not know the sender's account names, nicknames, online IDs, phone numbers, nor any other identifying information unless senders "reveal" themselves by "swiping up" in the app. *Id*.

According to the FAC, YOLO allegedly knew or should have known that "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." (ER-18–19). Despite allegedly knowing the "inherent dangers of anonymous messaging for teenagers," YOLO proceeded to make the YOLO anonymous messaging app widely available to the public and, according to the FAC, "did not put a plan in place to meaningfully prevent the foreseeable and expected harm that would result from having millions of teenagers use anonymous messaging every single day." (ER-18–19).

Thus, the Putative Class Members allege the YOLO app was defectively designed because its "key feature of anonymity" caused significant and foreseeable harm, given the anonymous messaging features' risk for being a "hotbed for bullying and harassment of minors." (ER-69–70).

---

message receivers to make public, non-anonymous posts as the only means to respond to an anonymous message sender. Opening Brief at p. 2, 4-5. Rather, the paragraphs to the FAC cited by the Putative Class Members in support of this claim (FAC at ¶¶56, 73, 98-99; Opening Brief at p. 5) allege the YOLO app allowed users to ask questions and send polls requests "on a completely anonymous basis" and allowed users "to chat with other users anonymously." (ER-39, ER-46).

The Putative Class Members also attempt to plead misrepresentation claims based on YOLO's alleged statements that it would take actions to implement certain safety measures. (ER-20). According to the FAC, YOLO allegedly made false statements because when users downloaded the YOLO app onto their phones, YOLO declared in pop-up messages that users would be "banned for any inappropriate usage" and if they "send harassing messages to our users, [their] identity will be revealed." *Id*. The FAC claims these statements were "false" because YOLO did not reveal the identities of users who harassed or engaged in other inappropriate conduct, or ban those users. (ER-20).

The crux of these allegations is that the Putative Class Members contend YOLO should have regulated what appeared on its app. Specifically, YOLO should have revealed the identities and banned users who sent harassing messages – the type of activity that boils down to a charge that YOLO had a duty to prevent users from posting objectionable content. (ER-20, ER-42, ER-81).

**2. <u>Carson Bride Used the YOLO app</u>**

The claims for Lead-Appellant, the Estate of Carson Bride, pertain to the anonymous messages that 16-year-old Carson Bride allegedly received through the YOLO app in 2020. (ER-24–25).

While using the YOLO app, the Putative Class Members allege Carson received 62 anonymous messages that included explicit content meant to humiliate.

(ER-50–53). Tragically, Carson took his own life in June 2020. (ER-21, ER-49). The Putative Class Members allege his "suicide was likely triggered by cyberbullying" from the harassing messages he received. (ER-21, ER-50).

### 3. Appellants Tyler Clementi Foundation, A.K., A.C., and A.O.

Appellant the Tyler Clementi Foundation (the "Foundation") is a non-profit organization registered in New York whose mission is to end online and offline bullying, harassment, and humiliation. (ER-27). The Foundation brought the action on behalf of itself and on behalf of its members, including its Youth Ambassador members in New York, who have allegedly used the YOLO app. (ER-27, ER-90–95). The organization asserts New York state claims related to false advertising and misrepresentation. (ER-27, ER-90–95).

On October 6, 2022, as part of the FAC, Appellants A.K., A.C., and A.O. were added to the pleading and alleged they suffered harm as a result of the anonymous messages received through the YOLO app. (ER-57–60).

### 4. Appellants' Complaint

On May 10, 2021, Plaintiffs Kristen Bride, the Estate of Carson Bride, and the Tyler Clementi Foundation filed the original Complaint against YOLO and against former Defendants Lightspace Inc. ("Lightspace") and Snap, Inc. ("Snap") in the U.S. District Court, Northern District of California. (ER-113). Within two days of the filing, Snap suspended the YOLO app. (ER-21–22).

The case was then transferred to the Central District on August 18, 2021. (ER ER-119). On June 17, 2022, Plaintiffs and Snap stipulated to Snap's dismissal with prejudice from this action. (ER-125). On June 27, 2022, the Putative Class Members filed their FAC that sought to bring a class action, and added three new Plaintiffs, A.K., A.C., and A.O. (ER-125).

The Putative Class Members' claims against YOLO fall under two overarching theories: product liability[3] and misrepresentation.[4] As to the product liability theory, they assert anonymous messaging apps are inherently dangerous (a putative "design defect") and, given the alleged lack of safeguards against the transmission of harmful anonymous messages, that YOLO can be sued for strict liability and negligence for permitting the Putative Class Members and other teenagers to use the app. (ER-69–70, ER-73–74, ER-76–78). As to the misrepresentation theory, the Putative Class Members allege YOLO made representations that it would take actions to implement so-called "safety measures," including revealing the identities and banning users who sent harassing messages,

[3] Counts 1 (strict liability / design defect), 2 (strict liability / failure to warn), 3 (negligence), 5 (unjust enrichment), 6 (Oregon Unlawful Trade Practices Act ("OUTPA")), 7 (N.Y. Gen. Bus. L. § 349), and 12 (California Unfair Competition Law ("UCL")). (ER-68–84, ER-86–83, ER-100–102).

[4] Counts 4 (fraudulent misrepresentation), 5 (negligent misrepresentation), 5 (unjust enrichment), 6 (OUTPA), 7-8 (N.Y. Gen. Bus. L. §§ 349–350), 9 (Colorado Consumer Protection Act), 10 (Pennsylvania Unfair Trade Practices Law), 11 (Minnesota False Statement in Advertising Act), and 12 (UCL). (ER-80–102).

that those representations were false, and that teenage users of YOLO's app (including Carson Bride) somehow relied on those representations. (ER-42, ER-81).

The Putative Class Members also assert unjust enrichment and state-specific claims predicated on allegations that YOLO committed false advertising/misrepresentation, or are otherwise coextensive with their product liability claims. (Appellee's Supplemental Excerpts of Record ("SER"), SER-20–21).

### 5. The District Court Grants YOLO's Motion to Dismiss the FAC With Prejudice

YOLO moved to dismiss all of the Putative Class Members' claims with prejudice pursuant to Federal Rule of Civil Procedure 12(b)(6) (the "Motion to Dismiss"). (ER-127, SER-64–97). The Motion to Dismiss was fully briefed and the District Court heard argument on January 5, 2023. (ER-127–128).

On January 10, 2023, the District Court entered an order granting YOLO's Motion to Dismiss the FAC in its entirety with prejudice. (ER-3–16, ER-128). In a detailed and thorough opinion spanning over 13 pages, the District Court held YOLO was immune from liability under Section 230 of the CDA on the basis that:

1) YOLO is an interactive computer service provider under Section 230. (ER-8–9).
2) The Putative Class Members cannot plead around YOLO's Section 230 immunity because, "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." (ER-9–10).

3) YOLO is not an information content provider under Section 230 because YOLO did not create or develop the harassing and explicit messages that led to the harm suffered by the Putative Class Members—the sending users did. And, the accusation here is fundamentally that YOLO should have monitored and curbed third-party content, which constitute claims that fall squarely within Section 230's broad grant of immunity. (ER-11–12).

Based on these reasons, the District Court dismissed all of Appellants' claims against YOLO with prejudice. (ER-3–16). This appeal followed.

## STANDARD OF REVIEW

Although YOLO agrees with the Putative Class Members' general statement of the standard of review, it omits certain elements that are noted below.

When presented with a motion to dismiss, a court must accept all facts alleged in a complaint as true and construe them in the light most favorable to the plaintiff, but it is not required "'to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences.'" *Cholla Ready Mix, Inc. v. Civish*, 382 F.3d 969, 978 (9th Cir. 2004) (quotation and citation omitted). Only a complaint that states a "plausible" claim for relief may survive a motion to

dismiss. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Plausibility only exists when the court may "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*.

The Court will affirm a dismissal for failure to state a claim where, as in this case, "there is no cognizable legal theory or an absence of sufficient facts to support a cognizable legal theory." *Los Angeles Lakers, Inc. v. Fed. Ins. Co*., 869 F.3d 795, 800 (9th Cir. 2017).

## SUMMARY OF THE ARGUMENT

The gravamen of the Putative Class Members' claims is that they suffered harm as a result of receiving anonymous messages from third-parties through the YOLO app (ER-21–22, ER-57–59, ER-60) and YOLO allegedly made inaccurate representations that it would take actions to implement safety measures, including revealing the identities and banning users who send harassing messages. (ER-18, ER-20). The legal principles that establish CDA immunity under these circumstances are well settled.

Section 230 of the CDA immunizes YOLO from all such claims because they seek to hold YOLO liable for third-party user generated content, to which YOLO made no material contribution, and for YOLO's allegedly insufficient screening and content-moderation. Accordingly, the District Court properly dismissed the Putative

Class Members' FAC in its entirety with prejudice. This appeal thus lacks merit for the following main reasons:

*First*, YOLO is immune from liability for the Putative Class Members' claims under the plain language of Section 230 of the CDA. YOLO is an interactive computer service that merely published the messages of its app users and did not materially contribute to them in any way. The Putative Class Members' attempts to salvage their claims by recasting the District Court's well-reasoned opinion as using a "but-for" publication test (i.e., that CDA immunity applies if a cause of action would not exist "but-for" content from a third party) is unavailing. Indeed, the District Court thoroughly and properly analyzed the duty element of each cause of action asserted by the Putative Class Members.

*Second*, the Putative Class Members seek to treat YOLO as a publisher of content generated by YOLO app users and their false advertising/misrepresentation claims are directed at YOLO's content moderation policies—which is exactly the kind of activity for which Congress intended Section 230 to provide immunity. The Putative Class Members' claims are essentially based on a pop-up in the YOLO app indicating: "YOLO is for positive feedback only. No bullying. If you send harassing messages to our users, your identity will be revealed." (ER-42). This statement is entirely regarding the general safety of the platform and the enforcement of YOLO's

guidelines as to third-party content. Claims based on such statements are routinely dismissed by courts under Section 230 immunity.

*Third,* no legal authority supports the Putative Class Members' notion that YOLO was an information content provider, and thereby lost its Section 230 immunity. YOLO passively displayed content by third parties and did not materially contribute to any harm —for which CDA immunity is warranted. Contrary to the Putative Class Members' claim, it is not enough that YOLO's platform design feature (i.e., anonymous messaging) allegedly contributed to the wrongful user content, which YOLO strenuously denies. Under settled precedent, no liability can attach unless the feature materially contributed to the bullying and harassing content. Here, the Putative Class Members do not and cannot state any plausible facts describing how YOLO might have created, materially contributed to, or facilitated any harmful content.

Indeed, this Court in *Dyroff* has already held an anonymity feature, alone, is a passive and content-neutral feature—with no inherent danger or predictability of harm. *See Dyroff v. Ultimate Software Grp., Inc*., 934 F.3d 1093, 1095-96 (9th Cir. 2019). The site in *Dyroff* was completely anonymous: users registered anonymously; the site collected no user identifying information; and, the founders specifically did not want to know any identifying information because anonymity fostered honesty and less inhibition. *Dyroff*, 934 F.3d at 1095. Despite such

"complete anonymity" this Court granted CDA immunity, correctly reasoning that the site's functions "were content-neutral tools used to facilitate communications." *Id*. at 1096.

*Fourth*, the Putative Class Members' attempts to plead around Section 230 are unavailing. The Putative Class Members try to circumvent the CDA by alleging they do not seek to hold YOLO liable as a publisher or speaker of content provided by third parties. However, all the alleged damages stem exclusively from the content of the third-party user communications. YOLO's product or its design are not inherently dangerous or defective; rather, it is the content of the user-generated communications that is at issue. The Putative Class Members do not (and cannot) allege that harm would have resulted from anonymous but non-harassing communications. Furthermore, the Putative Class Members cannot avoid Section 230 immunity by creatively attempting to recast their allegations as supposedly based upon YOLO's own conduct, such as an alleged failure to warn or alleged misrepresentations or false advertising regarding the treatment of harassment and bullying on the platform. The harm allegedly caused to the Putative Class Members is still based solely upon user-generated content and YOLO's allegedly deficient screening functions and content-moderation policy, all of which are fully immunized under Section 230.

For these reasons, as further explained below, this Court should affirm the District Court's order dismissing the FAC in its entirety with prejudice.

## ARGUMENT

### 1. The District Court Properly Dismissed Appellants' FAC Pursuant to the Plain Language of Section 230 of the CDA and its Decision is Supported by the Statutory Purpose of the CDA

According to settled principles, "[s]tatutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." *Engine Mfrs. Ass'n v. S. Coast Air Quality Mgmt. Dist.*, 541 U.S. 246, 252 (2004). If the "statutory text is plain and unambiguous" then the Court "must apply the statute according to its terms." *Carcieri v. Salazar*, 555 U.S. 379, 387 (2009). Indeed, when the statutory language is plain, courts "have no right to insert words and phrases, so as to incorporate in the statute a new and distinct provision." *United States v. Temple*, 105 U.S. 97, 99 (1881); *Guido v. Mount Lemmon Fire Dist.*, 859 F.3d 1168, 1175 (9th Cir. 2017) ("[I]t is not our role to choose what we think is the best policy outcome and to override the plain meaning of a statute[.]").

CDA Section 230(c)(1) states "[n]o provider . . . 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). "No cause of action

may be brought and no liability may be imposed under any State . . . law that is inconsistent with this section." Section 230(e)(3).

Congress enacted the CDA "to promote the free exchange of information and ideas over the Internet." *Carafano v. Metrosplash.com*, 339 F.3d 1119, 1122 (9th Cir. 2003). "Congress considered the weight of the speech interests implicated"—including how "the specter of tort liability . . . would have an obvious chilling effect" given the "staggering" amount of online speech—"and chose to immunize service providers to avoid any such restrictive effects." *Id.* at 1224. Based on these considerations, "courts have treated § 230(c) immunity as quite robust." *Id.* at 1223.

Here, the Putative Class Members seek to judicially limit Section 230's robust immunity by asserting YOLO should have no immunity unless it is "making good-faith efforts to prevent harm as 'Good Samaritans,'" supposedly per Congress' stated aim in enacting the CDA. Opening Brief at p. 21-22. They claim YOLO's conduct of designing an app with anonymity features and allegedly representing it had safety measures in place without actually implementing them is not consistent with a "Good Samaritan." *Id*.

However, while Sections (b)(4)–(5) of the CDA seek to enable filtering objectionable online materials and to ensure their enforcement, the policies underlying Section 230 are not limited to these goals. Nor can a court's interpretation of the CDA nullify its actual language or other stated goals. *Guido*,

859 F.3d at 1175 ("[I]t is not our role to choose what we think is the best policy outcome and to override the plain meaning of a statute[.]"). For example, Sections (b)(1)–(2) of the CDA state, "[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" and "preserve the vibrant and competitive free market that presently exists for the Internet . . . unfettered by Federal or State regulation." 47 U.S.C. § 230(b)(1)-(2). The CDA not only does not require Internet developers to meet the "Good Samaritan standard" as advanced and particularly defined by the Putative Class Members in this appeal; it even openly permits design features or related conduct that may not comply with such a subjectively heightened standard but nonetheless is (or was) part of the developing Internet.

Moreover, this Court's reasoning in *Dyroff* supports how the YOLO app's anonymity feature, alone, is actually passive and facially neutral—with no inherent danger or predictability of harm. In *Dyroff*, plaintiff sued an online messaging platform for her son's death after an anonymous message user through the online messaging platform directed her son to lethal drugs. Dyroff attempted to plead around CDA immunity by alleging her claims were based on the features and functions, including the algorithms of the website that recommended relevant users—and not third-party content. *Id.* at 1098. This Court rejected that argument. *Id.* at 1100. This Court reasoned that the CDA barred plaintiff's claims, which

"inherently require[d] the court to treat the defendant as the 'publisher or speaker'" of the messages at issue. *Id.* A plaintiff cannot circumvent § 230 immunity by focusing on an app's provision of "neutral tools that a user exploits" to create harmful content, rather than on the content itself. *Id.* at 1099. This Court also rejected plaintiff's attempt to circumvent the CDA (based on claims similar to those alleged here) through claims that the messaging platform should have known that drugs were sold on the platform, and that it supported and protected the conduct anyway through anonymity policies. *Id.* 1099.

Here, the Putative Class Members' allegations are nearly identical to those rejected in *Dyroff*: that YOLO's app was defectively designed because its "key feature of anonymity" caused significant and foreseeable harm, given the anonymous messaging features' risk for being a "hotbed for bullying and harassment of minors." (ER-69–70). This Court firmly rejected this line of argument in *Dyroff* by holding "Plaintiff's allegation that user anonymity equals promoting drug transactions is not plausible" and the "district court was right to dismiss all claims related to this supposed theory of liability because Ultimate Software is, as reasoned above, immune under Section 230." *Id*. at 1100.

In addition, the claim that YOLO allegedly failed to implement safety measures, such as banning users who sent harassing messages, goes toward YOLO's screening and content-moderation functions, which in turn are unequivocally

"perforce immune under Section 230." *Fair Hous. Council v. Roommates.com*, 521 F.3d 1157, 1179–80 (9th Cir. 2007) ("[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."); *924 Bel Air Rd., LLC v. Zillow Grp., Inc.*, 2020 WL 774354, at *4 (C.D. Cal. Feb. 18, 2020) ("Ultimately, Bel Air's allegations boil down to a charge that Zillow must prevent users from falsely claiming a Residence Page or posting false content. Yet, reviewing each user's activity and postings to ensure their accuracy is precisely the kind of activity for which Congress intended section 230 to provide immunity."); *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1103 (9th Cir. 2009), as amended (Sept. 28, 2009) ("[T]he duty that Barnes claims Yahoo violated derives from Yahoo's conduct as a publisher—the steps it allegedly took, but later supposedly abandoned, to de-publish the offensive profiles. It is because such conduct is *publishing conduct* that we have insisted that section 230 protects from liability 'any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online.'") (emphasis in original).

Thus, there is no basis to support the Putative Class Members' claims that YOLO's conduct is inconsistent with CDA policy goals, or the language of the CDA itself. The District Court properly found YOLO had CDA immunity under the plain language of Section 230 and did so by "apply[ing] the statute according to its terms." *Carcieri*, 555 U.S. at 387; ER– 6-11.

Rather, if the Court singles out YOLO and denies it Section 230 immunity as the Putative Class Members desire, then the Court would overturn years of CDA precedent upon which Internet developers have relied in their businesses while extra-Congressionally negating the CDA's goals "to promote the continued development of the Internet and other interactive computer services" and "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." 47 U.S.C. § 230(b)(1), (2). Simply put, the Court should not agree with the Putative Class Members to jeopardize the future of the Internet and the entire free competitive market based upon it—in direct contravention of federal legislation.

### 2. The District Court Properly Found That Section 230 of the CDA Immunizes YOLO from Liability for Appellants' Claims

Recognizing the Internet's continued growth was an important national interest, "Section 230 was enacted, in part, to maintain the robust nature of Internet communication, and accordingly, to keep government interference in the medium to a minimum." *Batzel v. Smith*, 333 F.3d 1018, 1027 (9th Cir. 2003) (quotation omitted). To fulfill this policy, Congress ensured that Section 230 "protects certain internet-based actors from certain kinds of lawsuits." *Barnes*, 570 F.3d at 1099.

Relevant here is the broad immunity that Section 230 confers on "providers of interactive computer services against liability arising from content created by third parties." *Roommates.com*, 521 F.3d at 1162; *Carafano*, 339 F.3d at 1123 ("§

230 provides broad immunity for publishing content provided primarily by third parties").

Under Section 230, "[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). A "publisher" has been defined as "'the reproducer of a work intended for public consumption' and also as 'one whose business is publication.'" *Barnes*, 570 F.3d at 1102. A publisher's responsibilities include "reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content." *Id*.

The immunity granted to interactive computer services under Section 230 addresses Congress' concern that litigation over published content would impair the goal of promoting free speech on the Internet. *See Batzel*, 333 F.3d at 1027-28. As this Court has recognized, "[m]aking interactive computer services and their users liable for the speech of third parties would severely restrict the information available on the Internet." *Id.* By enacting Section 230, Congress "sought to prevent lawsuits from shutting down websites and other services on the Internet." *Id.; see also Roommates.com*, 521 F.3d at 1174 ("We must keep firmly in mind that this is an immunity statute we are expounding, a provision enacted to protect websites against the evil of liability for failure to remove offensive content"); *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (Section 230 immunity resulted from

Congress' recognition of "the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium.").

Under this Court's three-prong test, Section 230's immunity protects from liability "(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. "When a plaintiff cannot allege enough facts to overcome Section 230 immunity, a plaintiff's claims should be dismissed." *Dyroff*, 934 F.3d at 1097 (citation omitted).

Here, all three prongs for Section 230 immunity are readily satisfied, as discussed in detail above and below. Given the essence of the Putative Class Members' claims seeking to hold YOLO liable for content created and published by anonymous third parties on its app, for designing an app with an anonymity feature that is passive and neutral with no inherent danger or predictability of harm, and for allegedly failing to implement safety measures that equate to YOLO's content-moderation policies, the District Court properly found that YOLO was entitled to Section 230 immunity.

#### *a. There is no Dispute That the YOLO app is an "interactive computer service" and Thus Satisfies the First Prong of the* Barnes *Test*

The CDA defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by

multiple users to a computer server." Section 230(f)(2). In *Lemmon v. Snap, Inc.*, this Court held Snapchat is an "interactive computer service" under the "expansive" definition of the term under the CDA. 995 F.3d 1085, 1091 (9th Cir. 2021). The Court reasoned that Snap, the creator, owner, and operator of the Snapchat app, is a provider of an "interactive computer service"—given that its Snapchat app permitted users to share photos and videos through Snapchat's servers and internet, necessarily enabling multiple user access to a computer service.

Here, as the FAC acknowledges, YOLO is the developer of the YOLO App, which provided its users with the YOLO service, an anonymous messaging app that allowed independent users to send messages, exchange questions and answers, and send polling requests to other users. (ER-27–28, ER-38). The YOLO app operated via "Snap Kits" and allowed multiple users to access to the YOLO app via Snapchat. *Id*. Therefore, for the same reasons articulated in *Lemmon*, YOLO is alleged to be and undisputedly is an "interactive computer service" under the CDA's expansive definition of the term. *See Lemmon*, 995 F.3d at 1092.

Furthermore, the Putative Class Members agree in their Opening Brief that the YOLO app meets the first prong of this Court's three-prong test for Section 230 immunity. Opening Brief at p. 17.

### *b. The District Court Properly Considered the Second Prong of the* **Barnes** *Test, and it is Satisfied Because Appellants Seek to Treat YOLO as a Publisher of Third-Party Content*

The District Court properly found that under the second prong of the *Barnes* test, what matters is if the Putative Class Members' claims "'inherently require[] the court to treat the defendant as the 'publisher or speaker' of content provided by another.'" (ER-8) (citing *Dyroff*, 934 F.3d at 1098 (alteration in original) (quoting *Barnes*, 570 F.3d at 1102)). Directly contrary to the Putative Class Members' assertion, the District Court did not use a "but-for" publication test in considering the second prong of the *Barnes* test. Instead, the District Court reached the conclusion that the Putative Class Members' product liability, negligence, and misrepresentation/false advertising claims were all barred by the CDA because the Putative Class Members "seek to hold Defendants liable based on content published by anonymous third parties on their applications," "treat Defendants as a publisher of content," and "Plaintiffs' claims are directed at Defendants' content moderation policies[.]" (ER-8, ER-12–14). Indeed, the District Court also thoroughly analyzed the duty element of each cause of action asserted by the Putative Class Members in its opinion:

- For the product liability claim based on how user anonymity is a defective design feature of YOLO's app, the District Court properly recognized that "[w]hile 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." (ER-9) (citing *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 District Court also recognized under *Dyroff* that the feature of anonymity in itself facilitates communication in a content-neutral fashion, and an anonymous posting feature cannot plausibly facilitate or promote objectionable content. (ER-9, ER-13).
- For the product liability claim based on failure to warn, the District Court found the Putative Class Members' theory depended on a close connection between the proposed warning and user-generated content such that it would improperly require YOLO to monitor and police third-party content. (ER-10, ER-12–13).
- For the negligence and state law claims predicated on the Putative Class Members' false advertising and misrepresentation allegations, the

> Court considered the Putative Class Members' argument that CDA immunity does not protect YOLO from its own alleged misrepresentations. The District Court ultimately agreed with YOLO that the claims are directed at YOLO's content moderation policies, and found "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." (ER-13).

The District Court held the Putative Class Members' claims fall squarely within Section 230(c)'s immunity provision because they seek to fault YOLO for its role as a publisher of information rather than an information content provider. The District Court's reasoning rested on the finding that YOLO "did not create or develop information" but rather "published information created or developed by third parties" and "[t]he accusation here is fundamentally that [Defendants] should have monitored and curbed third-party content." (ER-11) (quoting *Dyroff*, 934 F.3d at 1098 and *Jackson v. Airbnb, Inc*., 2022 WL 16753197, at *2 (C.D. Cal. Nov. 4, 2022).

Thus, the District Court did not base its holding of immunity solely by finding that had "third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable." (ER-11). Rather, put in the context that the Putative

Class Members tellingly omit, the District Court's main reasoning was "Defendants did not create or develop the harassing and explicit messages that led to the harm suffered by Plaintiffs; the sending users did" and the crux of the Putative Class Members' charge is that YOLO must monitor and curb third-party content. (ER-12). However, moderating and policing third party user activity and messages are precisely the kind of activity for which Congress intended Section 230 to provide immunity. *924 Bel Air Rd., LLC*, 2020 WL 774354, at *4; *Barnes*, 570 F.3d at 1103.

In addition, contrary to the Putative Class Members' argument, *Barnes* does not support the finding that the claims at issue derive from YOLO's role as a developer, seller, and advertiser of its anonymous messaging product, rather than a publisher of content.

First, this Court in *Barnes* held plaintiff's tort claim for negligent undertaking sought to treat Yahoo as a "publisher or speaker" of the objectionable online profiles posted by plaintiff's ex-boyfriend and which plaintiff sought Yahoo to take down. *Barnes*, 570 F.3d at 1102. Specifically, this Court found that "the duty that Barnes claims Yahoo violated derives from Yahoo's conduct as a publisher—the steps it allegedly took, but later supposedly abandoned, to de-publish the offensive profiles" but "removing content is something publishers do, and to impose liability on the basis of such conduct necessarily involves treating the liable party as a publisher of the content it failed to remove." *Id*. at 1103. Thus, *Barnes* actually supports finding

CDA immunity in favor of YOLO with respect to the Putative Class Members' products liability and tort claims premised on YOLO's alleged failure to remove offensive content or ban users who sent harassing messages, as such claims "necessarily involve[] treating the liable party as a publisher of the content it failed to remove." *Id.*

Second, *Barnes* is otherwise distinguishable. This Court found no CDA immunity as to a different claim for promissory estoppel/breach-of-promise, because "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." *Id.* 1107, 1109. Here, however, there are no contractual claims at issue and the Putative Class Members had the opportunity to amend their complaint. Instead, they chose only to assert claims for product liability, negligence, fraudulent and negligent misrepresentation, unjust enrichment, and state-law claims predicated on false advertising or misrepresentations. Since the Putative Class Members twice chose **not** to sue under any contractual theory, they should be precluded from doing so with respect to allegations based on YOLO's representations in its Terms of Use and other policies.

Further, the Putative Class Members specifically raised the infancy defense to disaffirm the YOLO app's Terms of Use. (ER-50). Case law is clear that a minor cannot inequitably retain the benefits of a contract (and sue under it) while reneging

on the burdens and conditions attached to the benefits. *Doe #1 v. Coll. Bd.*, 440 F. Supp. 3d 349, 356 (S.D.N.Y. 2020) ("Even if there were procedural unconscionability due to Plaintiffs' age, Plaintiffs are not entitled to argue both that Defendant breached the T&C and seek the release of the May 2019 exam scores, while also claiming the Arbitration Provision was unconscionable.") (citing *I.C. ex rel. Solovsky v. Delta Galil USA*, 135 F. Supp. 3d 196, 209 (S.D.N.Y. 2015) (observing under New York law "[t]he privilege of infancy is to be used as a shield, not as a sword")); *Holland v. Univ. Underwriters Ins. Co.*, 270 Cal.App.2d 417 (1969) (California law is in accord with "the equitable principle that minors, if they would disaffirm a contract, must disaffirm the entire contract, not just the irksome portions."); *Peers v. McLaughlin*, 88 Cal. 294, 299 (1891) ("[Minors] must either accept or repudiate the entire contract, and they cannot retain [the contract's] fruits and at the same time deny its obligations.").

Third and lastly, the District Court's ruling is consistent with *Barnes*' guidance to examine the duty element for each cause of action, as detailed above. 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. The District Court properly recognized that the YOLO app is being sued for publishing third-party content, for its passivity, and the mere fact that it contained an anonymity feature without policing against harmful content generated by third-party users.

(ER-23–24, ER-27–28, ER-37, ER-42). At its core, the Putative Class Members' charge that YOLO failed to implement safety features (i.e., ban users who sent harassing messages) is directed at YOLO's screening and content-moderation functions. Accordingly, the District Court reasonably found "[i]mposing such a duty would necessarily require [Defendants] to monitor third-party content." (ER-11) (citation omitted).

Of course, this Court (among many others) has found CDA immunity applies when the claims boil down to failing to monitor, exclude, or remove objectionable third-party content. *See Al-Ahmed v. Twitter, Inc.*, 603 F. Supp. 3d 857, 881 (N.D. Cal. 2022), *appeal dismissed*, 2022 WL 4352712 (9th Cir. July 7, 2022) ("As discussed above, removal of posts and accounts of a user is generally considered as treating the information content provider as a publisher.") (citing *Barnes*, 570 F.3d at 1109) (finding that the removal of social media content falls under Section 230(c)(1) and *King v. Facebook, Inc.*, 572 F.Supp.3d 776, 780-81 (N.D. Cal. 2021) (finding that claims relating to disabling of accounts fall under Section 230(c)(1))); *924 Bel Air Rd., LLC*, 2020 WL 774354, at *4 ("Ultimately, Bel Air's allegations boil down to a charge that Zillow must prevent users from falsely claiming a Residence Page or posting false content. Yet, reviewing each user's activity and postings to ensure their accuracy is precisely the kind of activity for which Congress intended section 230 to provide immunity."); *Murphy v. Twitter, Inc.*, 60

Cal.App.5th 12, 27 (2021) ("Courts have routinely rejected a wide variety of civil claims like Murphy's that seek to hold interactive computer services liable for removing or blocking content or suspending or deleting accounts (or failing to do so) on the grounds they are barred by the CDA.") (citing *Doe II v. MySpace Inc*., 175 Cal.App.4th 561, 573 (§ 230 immunity barred tort claims based on social networking website's decisions whether "to restrict or make available" minors' profiles)).

Furthermore, the Putative Class Members' position that this case is similar to *HomeAway.com, Inc. v. City of Santa Monica* was already rejected by this Court in *Dyroff* when it disposed of a similar claim. In *Dyroff*, this Court recognized defendant Ultimate Software was not an information content provider because the platform "did not create or develop the posts that led to Greer's death. Rather, it was Greer, himself, who posted 'where can i [sic] score heroin in jacksonville, fl' on Experience Project. And it was the drug dealer, Margenat-Castro, who posted in response to Greer's post." *Dyroff*, 934 F.3d at 1098. This Court also recognized that Dyroff (like the Putative Class Members) was attempting to plead around CDA immunity by alleging her claims were based on the features and functions, including the algorithms of the website that recommended relevant users—and not third-party content. *Id*. And, the Court rejected that argument. *Id*. at 1100. In its reasoning, this Court found the CDA barred Dyroff's claims, which "inherently require[d] the

court to treat the defendant as the 'publisher or speaker'" of the messages at issue. *Id.* A plaintiff cannot circumvent § 230 immunity by focusing on an app's provision of "neutral tools that a user exploits" to create harmful content, rather than on the content itself. *Id.* at 1099.

The Court also rejected Dyroff's attempt to circumvent the CDA (based on claims similar to those alleged here (ER-69–70) through claims that the messaging platform should have known that drugs were sold on the platform but it supported/protected the conduct via anonymity policies. *Dyroff*, 934 F.3d at 1099-1100 ("Plaintiff's allegation that user anonymity equals promoting drug transactions is not plausible. The district court was right to dismiss all claims related to this supposed theory of liability because Ultimate Software is, as reasoned above, immune under Section 230.") (citation omitted).

Based on the above, this Court in *Dyroff* found its "recent decision, *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676 (9th Cir. 2019) is of no help to Plaintiff." *Id*. at 1098. The Court explained in *HomeAway*, the City of Santa Monica required short-term vacation rentals to be licensed and imposed liability on vacation rental hosting platforms—HomeAway.com and Airbnb—that facilitated unlicensed short-term vacation rentals. *Id*. This Court held HomeAway.com and Airbnb did not meet the second prong of the *Barnes* test because the Santa Monica ordinance did not "proscribe, mandate, or even discuss the content of the [website]

listings," and required only that the website's transactions involve licensed properties. *Id*. ("In other words, the vacation rental platforms did not face liability for the content of their listings; rather liability arose from facilitating unlicensed booking transactions.").

However, the Court recognized that was not the situation in *Dyroff*. *Id*. Defendant Ultimate Software satisfied the second prong of the *Barnes* test because it was facing liability for publishing third-party content—it did not create or develop content. *Id*. The same is true in this case: the YOLO app was allegedly defectively designed because its "key feature of anonymity" caused significant and foreseeable harm, given the anonymous messaging features' alleged risk for being a "hotbed for bullying and harassment of minors." (ER-69–70). Consistent with the reasoning in *Dyroff*, the Putative Class Members cannot circumvent the CDA by focusing on the YOLO app's anonymity feature, which is a neutral tool that the user exploits in creating harmful content. *See* Dyroff, 934 F.3d at 1100. Here, the Putative Class Members' claims inherently require the Court to treat YOLO as the "publisher or speaker" of content provided by another. *Dyroff*, 934 F.3d at 1098 ("We have held that what matters is whether the claims 'inherently require[ ] the court to treat the defendant as the 'publisher or speaker' of content provided by another.'" If they do, then Section 230(c)(1) provides immunity from liability.") (citations omitted).

Thus, the Putative Class Members' attempt to reframe the District Court's sound analysis as using a "but-for" third-party content publication test, or failing to examine the duty element of each cause of action, rings hollow.

i. The District Court Drew All Factual Inferences In Appellants' Favor

Next, the Putative Class Members make the baseless claim that the District Court failed to accept the FAC's factual allegations as true and failed to draw all factual inferences in their favor. Contrary to the Putative Class Members' claim, it is them (and not the District Court) that is forcing factual inferences not asserted or contemplated in the FAC.

First, based on the Putative Class Members' theory that YOLO should be held liable for publishing content created by third parties that is allegedly harmful because the speakers are anonymous, the District Court logically inferred that imposing such a duty would necessarily require YOLO to monitor third-party content as it would need to ensure each user's post on its application is traceable to a specifically identifiable person. Contrary to the Putative Class Members' new appellate contentions, the FAC does **not** allege that YOLO app users are already traceable and identifiable. As cited by the Putative Class Members, Paragraph 26 of the FAC merely alleges the YOLO app is "designed to allow its users to send messages to each other anonymously" and the receiver of a message does not know the sender's identifying information unless the sender reveals themselves by "swiping up" in the

app. (ER-27–28). That is not at all the same as alleging YOLO already has the actual ability to trace and identify each user on the app. In addition, nowhere in the FAC do the Putative Class Members assert YOLO had the actual ability to remove a user's anonymity mode.

Second, the Putative Class Members argue for the first time that YOLO could have "simply allowed receivers of anonymous messages to remove their sender's anonymity and reveal their identity" with absolutely no facts to support this assertion in their FAC. Opening Brief at p. 31. Even setting aside the Putative Class Members' improper assertion that was never raised in their FAC or before the District Court, such conduct (to permit or remove anonymity) would still constitute "decisions about the structure and operation of a website [and] are content-based decisions" under Section 230. *See Fields*, 217 F. Supp. 3d at 1124 (noting courts have held such content-based decisions include "the option to anonymize email addresses, [and the] acceptance of anonymous payments") (citing *Backpage.com, LLC*, 817 F.3d at 20); *see also Lewis*, 461 F. Supp. 3d at 954.

In the First Circuit's *Backpage.com, LLC* decision, the court held that Section 230(c)(1) immunity extended to "the formulation of precisely [this] sort of website policies and practices"—i.e., ones that "reflect choices about what content can appear on the website and in what form." 817 F.3d at 21. Further, the court specifically held that Backpage's "provision of e-mail anonymization" and other

messaging features were "publisher choices entitled to the protections of section 230(c)(1)." *Id*. at 21. Accordingly, even though the Putative Class Members' fabricated contention must be ignored, it does not permit the FAC to survive anyway.

In any event, the District Court's reasoning did not hinge on YOLO's actual ability to trace and identify each user to their posts; rather, the District Court found the Putative Class Members' claims would force YOLO to monitor and police content. That type of activity – to review, restrict, or make available certain content – is precisely the kind for which Congress intended to provide Section 230 immunity. *Al-Ahmed*, 603 F. Supp. 3d at 881 ("removal of posts and accounts of a user is generally considered as treating the information content provider as a publisher.") (citations omitted); *Barnes*, 570 F.3d at 1109 (finding that the removal of social media content falls under Section 230(c)(1)); *924 Bel Air Rd., LLC*, 2020 WL 774354, at *4 ("Bel Air's allegations boil down to a charge that Zillow must prevent users from falsely claiming a Residence Page or posting false content. Yet, reviewing each user's activity and postings to ensure their accuracy is precisely the kind of activity for which Congress intended section 230 to provide immunity.").

In sum, the nature and breadth of the Putative Class Members' allegations in the FAC confirm that they seek to hold YOLO liable for publishing third-party content rather than for content YOLO created or developed. Here, the crux of the Putative Class Members' claims is that the harassing, anonymous messages Carson,

A.K., A.C., and A.O. received through the YOLO app caused Carson to take his own life and resulted in harm to A.K., A.C., A.O. The publisher-treatment requirement is therefore satisfied, and Courts have granted CDA immunity in numerous instances similar to this one. *See, e.g.*, *Dyroff*, 934 F.3d at 1097–98 (requirement satisfied where claims against website operator were based on messages exchanged through users/third-parties over website); *Carafano*, 339 F.3d at 1122, 1124 (same where claims against dating website were based on an anonymous user creating a fake dating profile that impersonated the plaintiff). Thus, the second prong of the *Barnes* test is also satisfied.

ii. The Electronic Privacy Information Center is Asking the Court to Limit Section 230's Robust Immunity by Adopting an Unprecedented Standard

To the extent this Court considers the Electronic Privacy Information Center and Fairplay's ("EPIC") amicus brief, EPIC similarly seeks to limit Section 230's robust immunity by asking this Court to adopt a legal requirement never previously recognized. Specifically, EPIC asserts "Section 230 allows claims that would not require the defendant to monitor, edit, or remove third-party content to avoid liability" such that the Court "must determine whether engaging in publishing activities is the *only* way to fulfill the alleged duty," and if not, then the claim should not be barred under the CDA. Amicus Brief at 14-16 (emphasis in original). EPIC is incorrect. In *Dyroff*, this Court found Ultimate Software satisfied the second

prong of the *Barnes* test as plaintiff's claims inherently required the Court to treat Ultimate Software as a publisher or speaker of third-party content. 93 F.3d at 1098-99. In reaching that conclusion, the Court did **not** hold Dyroff's claims "required the defendant to monitor, edit, or remove third-party content to avoid liability." So long as a plaintiff's claim treats an interactive computer service, like YOLO, as a publisher or speaker of third-party content, then the second prong of the *Barnes* test is met. *Dyroff*, 93 F.3d at 1098-99.

***c. The District Court Properly Considered the Third Prong of the* Barnes *Test, and it is Satisfied Because the YOLO App's Anonymity Design is Passive and Neutral With no Inherent Danger While YOLO did not Materially Contribute to the Alleged Objectionable Third-Party Content***

In a further effort to avoid Section 230 immunity, the Putative Class Members try to characterize YOLO as an information content provider by fundamentally misinterpreting this Court's prior rulings. Specifically, the Putative Class Members assert "whether CDA immunity applies turns on whether the operative pleading alleges that the internet company's tool or product at issue is content-neutral." Opening Brief at p. 36. The Putative Class Members overreach by claiming the definition of a neutral tool is something that "does not impact the substance of the created content" such that if "a user would feel obliged to change the content of the speech based on the way that the tool is designed [] then it is not content-neutral." *Id*. at 36-37. According to the Putative Class Members, the District Court erred by

ignoring facts alleging YOLO's product design (anonymity tool) altered the way 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. *Id*. at 37.

However, this interpretation of this Court's precedent and other case law goes too far as it would contradict the very cases cited by the Putative Class Members. For instance, *Dyroff* involved a platform's algorithm recommending a user connect with a drug dealer and notified the dealer of the recommended connection, whereupon the user and dealer then used the defendant's website to arrange a drug transaction. *Dyroff*, 934 F.2d 1095, 1097-1098. Clearly, the platform algorithm in *Dyroff* impacted the substance of the content created between the user and dealer, and changed the content of speech based on the way the algorithm was designed. But in finding the platform immune from suit under Section 230, this Court explained that while the "recommendation and notification functions helped facilitate this user-to-user communication," the platform "did not materially contribute, as Plaintiff argues, to the alleged unlawfulness of the content." *Id*. at 1099 (citing *Roommates.com*, 521 F.3d at 1175).

In *Roommates.com*, this Court adopted a "material contribution" test in defining when a website "develops" information:

> [W]e interpret the term "development" as referring not merely to augmenting the content generally, but to materially contributing to its

> alleged unlawfulness. In other words, a website helps to develop unlawful content, and thus falls within the exception to section 230 [immunity], if it contributes materially to the alleged illegality of the conduct.

521 F.3d at 1167-68.

Under this test, the website in *Roommates.com* clearly was the developer of the content at issue. *Id*. at 1170. Not only did the website prepare the allegedly discriminatory questions and answer choices that served as the focus of the registration process and, ultimately, became the cornerstone of each subscriber's online profile, it designed the search function to guide users through allegedly discriminatory criteria. *Id*. at 1164, 1167. Its search system steered users based on preferences and personal characteristics that the platform forced subscribers to disclose—and, in doing so, specifically differed from a generic search engine like Google. *Id*. at 1167. The website then allegedly hid housing opportunities from subscribers based on their responses to the questions it unlawfully required them to answer about protected characteristics. *Id*. at 1169. Thus, because of the website's "direct and palpable" role in the alleged discriminatory filtering process, this Court concluded that it "forfeit[ed] any immunity to which it was otherwise entitled under section 230." *Roommates.com*, 521 F.3d at 1170

In contrast, this Court in *Roommates.com* identified the type of conduct that does not constitute the "development" of content under section 230. *Roommates.com, LLC*, 521 F.3d at 1169. For example, a website does not become

a developer when it provides neutral tools that an individual uses to perform illicit searches. *Id*. In sum, a website enjoys Section 230 immunity in that case because its users are responsible for generating the content, and it has made no material contribution to the alleged illegality. *Id*. Thus, contrary to the Putative Class Members' claim, it is not enough that YOLO's platform design feature (i.e., anonymous messaging) indirectly contributed to the wrongful user content, which YOLO strenuously denies, the feature had to materially contribute to the bullying and harassing content.

Here, YOLO passively displayed content by third parties and did not materially contribute to any harm—for which CDA immunity is warranted. *See Roommates.com, LLC*, 521 F.3d at 1162. Neither the Putative Class Members' FAC nor their Opening Brief contain any plausible facts or reasoning describing how YOLO created, materially contributed to, or facilitated harmful content. Rather, YOLO is being sued for its passivity, and the mere fact that its app contained an anonymity feature and lacked policing against content generated by third-party users. (ER-23–24, ER-27–28, ER-37, ER-42). Accordingly, Plaintiffs' reliance upon *Roommates.com* is entirely misplaced.

CDA immunity must be granted because the Putative Class Members do not—and under no construct of the facts can—plead that YOLO, itself, created the harmful content alleged in this lawsuit or that it required users to post specific content, made

suggestions regarding the content of potential user posts, or contributed to making unlawful or objectionable user posts. *See Dyroff*, 934 F.3d at 1099; *Carafano*, 339 F.3d at 1124 (reasoning that platform receives full immunity so long as a third party willingly provides the essential published content).

The YOLO app's anonymity feature was a facially neutral tool, but the Putative Class Members seek to avoid controlling precedent by claiming a distinction where none exists. They claim *Dyroff* is inapplicable because users in that case posted under pseudonyms whereas, for the first time, the Putative Class Members are now claiming the YOLO app "was designed to give a one-sided privilege to keep the message sender anonymous, while the message receiver was identifiable." Opening Brief at p. 38-39. However, the Putative Class Members are incorrect on multiple grounds.

First, the Putative Class Members have waived and are estopped from making any argument that the YOLO app was a "one-sided, anonymous messaging app." In the District Court, the Putative Class Members failed to raise this argument. Instead, the Putative Class Members in their own opposition brief to the Motion to Dismiss claimed that the YOLO app provided "complete anonymity." (SER-41–42). Thus, the Putative Class Members should not be allowed to contradictorily raise this issue after failing to preserve it.

Second, even if this Court entertains the Putative Class Members' new argument, the FAC conspicuously omitted any factual allegation that the app was designed to be a one-sided, anonymous messaging app that required message receivers to make public, non-anonymous posts as the only means to respond to an anonymous message sender. Opening Brief at p. 2, 4-5, 38-39. Indeed, none of the paragraphs in the FAC cited by the Putative Class Members (¶¶26, 56, 73, 96, 98-99; Opening Brief at p. 5) even come close to suggesting the app was a one-sided, anonymous messaging app. Rather, the FAC alleged the YOLO app allowed users to ask questions and send polls requests "on a completely anonymous basis" and allowed users "to chat with other users anonymously." (ER-27–28, ER-39, ER-46).

Third, the Putative Class Members misconstrue the facts in *Dyroff* and twist it by saying users in that case posted under pseudonyms. Rather, the site in *Dyroff* was completely anonymous: users registered anonymously; the site collected no user identifying information; and, the founders specifically did not want to know any identifying information because anonymity fostered honesty and less inhibition. *See Dyroff*, 934 F.3d at 1095. Notwithstanding such "complete anonymity" in *Dyroff* this Court granted CDA immunity, reasoning that the site's functions "were content-neutral tools used to facilitate communications." *Id.* at 1096. Like *Dyroff*, YOLO's anonymity feature was a facially neutral tool which was "meant to facilitate the communication and content of others." *See id.* "[A] website does not become a

developer of content when it provides neutral tools that a user exploits" to create harmful content. *Id.* at 1099; *Roommates.com, LLC,* 521 F.3d at 1169.

In a further attempt at pleading around the CDA, the Putative Class Members argue that YOLO's anonymity feature was distinct because users did not have the ability to reveal the identities of the bad actors. Opening Brief at p. 2, 4-5, 38-39. This is nothing more than indirect way of alleging there were no sufficient safeguards (i.e., the ability to contact or investigate the third-party user generating harmful comments), which is the kind of activity for which Congress intended section 230 to provide immunity. *See In re Facebook, Inc.*, 2021 WL 2603687, at *9–11 (Tex. June 25, 2021) (holding that § 230(c)(1) barred product-liability claim premised on Facebook platform's allegedly insufficient safety measures); *Herrick v. Grindr, LLC,* 306 F.Supp.3d 579, 589 (S.D.N.Y. 2018), aff'd 765 F.App'x. 586 (2d Cir. 2019) (CDA barred claims because defendant could not be held liable for "tools and functionality that are available equally to bad actors and [to] the app's intended users" and claiming lack of adequate safeguards is just another way of asserting that it is liable because it fails to police and remove impersonating content); *Al-Ahmed v. Twitter, Inc.*, 603 F. Supp. 3d 857, 881 (N.D. Cal. 2022), *appeal dismissed*, 2022 WL 4352712 (9th Cir. July 7, 2022)) ("removal of posts and accounts of a user is generally considered as treating the information content provider as a publisher."); *Gentry v. eBay, Inc.*, 99 Cal.App.4th 816, 833–34 (2002) (holding that plaintiffs

could not avoid § 230 by attacking the structure of defendant's "safety program"); *924 Bel Air Rd., LLC*, 2020 WL 774354, at *4 ("reviewing each user's activity and postings to ensure their accuracy is precisely the kind of activity for which Congress intended section 230 to provide immunity.").

Thus, this Court should affirm the District Court's ruling that CDA immunity applies in this case, as the third prong of the *Barnes* test is also satisfied. The YOLO app's anonymity design is passive and neutral with no inherent danger, and did not materially contribute to the alleged objectionable third-party content.

### 3. Appellants' Efforts to Plead Around Section 230 are Unavailing, and the CDA Bars Appellants' Claims

The Putative Class Members additionally try to circumvent the CDA by declaring they do not seek to hold YOLO liable as a publisher or speaker of content provided by third parties. However, all the alleged damages stem from the content of the third-party communications. YOLO's product or its design is not inherently dangerous or defective; rather, it is the content of the user-generated communications that is at issue. The Putative Class Members do not (and cannot) allege that harm would have resulted from anonymous but non-harassing communications.

The Putative Class Members try to dodge CDA immunity by analogizing their claims to *Lemmon v. Snap* and *A.M. v. Omegle.com, LLC*, 2022 WL 2713721 (D.

Or. July 13, 2022). However, the present case is fundamentally different from *Lemmon* and *Omegle.com*—in which the courts declined to grant CDA immunity where the ***inherently dangerous features*** of the products were at issue, and **not the substance and content of the third-party generated messages.**

In *Lemmon*, plaintiffs alleged negligent design, claiming Snap built a "speed filter" function allowing users to record their driving speeds, along with "an incentive system within Snapchat that encouraged its users to pursue unknown achievements and rewards" by driving at unsafe speeds. *Lemmon*, 995 F.3d at 1087, 1091–92. Plaintiffs alleged that these functions, coupled with the incentive system, encouraged their sons to drive at high speeds, ultimately resulting in their deaths. *Id.* 1088–89. This Court held plaintiffs' negligent design claim was not subject to CDA immunity given the plaintiffs' claim depended not on the content of the speaker; rather, on the "the danger in the speeding" allegedly encouraged by the speed filter and incentive system. *Id.* at 1092-1093. 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 claims rested on "nothing more than Snap's 'own acts'" and were not based on "information provided by another content provider." *Id*. at 1094. In contrast, the Court further reasoned:

> Parents would not be permitted under § 230(c)(1) to fault Snap for publishing other Snapchat-user content (e.g., snaps of friends speeding dangerously) that

> may have incentivized the boys to engage in dangerous behavior. For attempting to hold Snap liable using such evidence would treat Snap as a publisher of third-party content, contrary to our holding here.

*Lemmon*, 995 F.3d at 1093 n.4. The claims here are precisely the kind this Court in *Lemmon* identified as falling *within* the § 230(c)(1) immunity. The claims against YOLO are based upon publishing of YOLO's user content that allegedly caused harm to Appellants. (ER-49–50, ER-57–60). These claims are distinguishable from *Lemmon*, given that, here, the user-generated messages caused harm—and not YOLO's own acts. *Lemmon,* 995 F.3d at 1087, 1094. The alleged design defect here—anonymous messaging—is a facially neutral feature that is not inherently dangerous (unlike Snap's built-in speed filter and incentivization for fast driving, which is inherently dangerous) and can only become so through harmful user-generated content. Thus, because the alleged harm that flows from the anonymity feature of YOLO's app is directly related to contents of third-party messages, CDA immunity applies. *See Doe v. Twitter, Inc.*, 555 F. Supp. 3d 889, 930 (N.D. Cal. 2021) (product liability claim barred by the CDA because the harm that flows from the alleged design flaw is "directly related to the posting of third-party content on Twitter" and is thus distinguishable from *Lemmon*).

*Omegle.com* is also inapposite. In *Omegle.com*, the plaintiff sued an online chat room for randomly pairing a minor with a man in his late thirties, resulting the minor's exploitation and forced transmission of pornographic material to the adult

man. *Omegle.com*, 2022 WL 2713721, at *1. The court declined to extend CDA immunity to the online chat room, because the case did not rest on Omegle's publication of third-party content (i.e., the forced pornographic images, chats, or videos of the minor)—and, instead, concerned the actual ***inherently dangerous*** feature that caused an "interaction between an eleven-year-old girl and a sexual predator in his late thirties." *Id.* at 4. ("Plaintiff's contention is that the product is designed a way that connects individuals who should not be connected (minor children and adult men) and that it does so before any content is exchanged between them.").

This case is therefore distinguishable from both *Lemmon* and *Omegle.com.* The harm alleged in *Lemmon* and *Omegle.com* was a "predictable consequence" of ***an inherently dangerous*** product feature and "a clear example of a claim that simply does not rest on third-party content": In *Lemmon*, it was the built-in speed filter and incentive system which predictably encouraged speeding and obviously dangerous behavior, *Lemmon*, 995 F.3d at 1087, 1091–92; and, in *Omegle.com* it was the product feature that paired a minor with an adult in a chatroom and it did so before any content was exchanged between them. *Omegle.com*, 2022 WL 2713721, at *1. The actual content of the posts (i.e., speeding posts or pornographic material of a minor) was not at issue in those cases.

Here, YOLO's anonymity feature is passive and facially neutral—with no inherent danger or predictability of harm. *See Dyroff*, 934 F.3d at 1096. Absent exploitation by third-party users, anonymous messaging is entirely innocuous—and no novelty, considering the internet. *See id.* at 1099. In fact, all specific details of the harm alleged are comprised of third-party generated comments published on YOLO's platform, and the CDA precludes such claims. (ER-50–52, ER-56–60); s*ee Lemmon*, 995 F.3d at 1087, 1093 n. 4.

***a. Appellants' Design Defect Claim is Barred by the CDA***

The Putative Class Members try to escape CDA immunity by attempting to plead around Section 230 by alleging negligent design/design defect claims. But no matter how artfully pled, courts have repeatedly rejected similar attempts and the following cases are particularly illustrative.

First, as discussed at length, in *Dyroff*, plaintiff attempted to plead around CDA immunity by alleging that her claims were based on the features and functions, including the algorithms of the website that recommended relevant users—and not third-party content. 934 F.3d at 1098. This Court rejected that argument. *Id.* at 1100. The Court reasoned that the CDA barred plaintiff's claims, which "inherently require[d] the court to treat the defendant as the 'publisher or speaker'" of the messages at issue. *Id.* A plaintiff cannot circumvent § 230 immunity by focusing on an app's provision of "neutral tools that a user exploits" to create harmful content,

rather than on the content itself. *Id.* at 1099. The Court also rejected Dyroff's attempt to circumvent the CDA (based on claims similar to those alleged here, *e.g.* ER-69–70), through claims that the messaging platform should have known drugs were sold on the platform and that it supported and protected the conduct through anonymity policies. *Id*. 1099.

Similarly, in *Black v. Google, Inc*., the federal court held "[a] fair reading of Plaintiffs' complaint demonstrates that they seek to impose liability on Defendant for content created by an anonymous third party" and that based on these allegations, Google was immune from suit under Section 230. 2010 WL 3222147, at *2–3 (N.D. Cal. Aug. 13, 2010), *aff'd*, 457 F. App'x 622 (9th Cir. 2011). The lawsuit was based on an allegedly defamatory and anonymous comment posted on the Google website that caused plaintiffs' business to suffer damages, but plaintiffs did not allege Google was its author. *Id*. The plaintiffs argued CDA immunity did not apply "because their claims are based on Defendant's 'programming,' not third-party content" and seemed to be referring to the source code underlying the services offered on Google's website. *Id*. at *3. The court in *Black* rejected this argument finding "Defendant's programming does not transform it into the creator of the offending comment. Indeed, several courts have considered and rejected theories that an interactive computer service could be held liable merely because its programming facilitated the creation of the content at issue." *Id*. (citations omitted).

Second, in the First Circuit's *Jane Doe No. 1 v. Backpage.com, LLC* decision, plaintiffs sued the website operator, claiming that the ads posted on the site led them to become sex-trafficking victims. 817 F.3d 12, 16 (1st Cir. 2016). Plaintiffs argued that Section 230(c)(1) did not apply because they did not seek to hold the operator liable for the ads themselves but rather for choices it had made about the website, such as "rules about which terms are permitted or not permitted…, the lack of controls on the display of phone numbers, the option to anonymize e-mail addresses, …[and] the website's reaction after a forbidden term is entered into an advertisement." *Id.*at 20. The First Circuit rejected plaintiffs' argument, holding that Section 230(c)(1) immunity extended to "the formulation of precisely [this] sort of website policies and practices"—*i.e.*, ones that "reflect choices about what content can appear on the website and in what form." 817 F.3d at 21. Further, the court specifically held that Backpage's "provision of e-mail anonymization" and other messaging features were "publisher choices entitled to the protections of section 230(c)(1)." *Id.* at 21.

Third, in the Second Circuit's *Herrick v. Grindr, LLC* decision, the plaintiff alleged a dating app contained features like geolocation that could be easily misused to harass, and did not contain safety features that would have enabled the removal of impersonating accounts. 306 F.Supp.3d at 586–88. The *Herrick* court applied Section 230(c)(1) to bar the claims, finding that defendant could not be held liable

for "tools and functionality that are available equally to bad actors and [to] the app's intended users." 306 F. Supp.3d at 589. And, plaintiff's claims alleging that the app had "failed to incorporate adequate protections" against fake accounts were "just another way of asserting that Grindr is liable because it fails to police and remove impersonating content." *Id.* at 590.

Courts have also generally rejected attempts by plaintiffs to plead around Section 230(c)(1) by alleging that their claims are based not on the allegedly harmful content itself but on a defendant's failure to implement safeguards to prevent such content. *In re Facebook, Inc*., 2021 WL 2603687, at *9–11 (holding that § 230(c)(1) barred product-liability claim premised on Facebook platform's allegedly insufficient safety measures); *Doe v. MySpace, Inc.*, 528 F.3d 413, 419–420 (5th Cir. 2008) (affirming dismissal under § 230(c)(1) of claim based on failure to implement measures to prevent predators from communicating with minors on MySpace); *Doe II*, 175 Cal.App.4th at 573.

***b. Appellants' Failure to Warn Claim is Barred by the CDA***

The Putative Class Members failure to warn claim is based on YOLO's alleged failure to warn about the "well-known and foreseeable dangers of anonymous messaging for minors." (ER-74). This is another effort at circumventing

the CDA by attempting to fit under *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 851 (9th Cir. 2016).

*Internet Brands* is inapposite. In *Internet Brands*, a model brought a failure to warn claim against the website operator after two website users lured her into a fake audition and raped her. *Id*. at 848. This Court held the CDA *did not* bar the model's claim because her claim had "nothing to do with Internet Brands' efforts, or lack thereof, to edit, monitor, or remove user generated content," and that no messages or content on defendant's site were at issue. *Id*. at 852. Rather, the model's claim was based on the website operator's knowledge, obtained from sources outside of the website, of the website users' rape scheme. *See id*. at 848-49, 852-53.

The *Herrick* court rejected a similar attempt to avoid Section 230(c)(1) based on *Internet Brands*. The court found that *Internet Brands*' carve-out did not apply because the plaintiff's "failure to warn claim depend[ed] on a close connection between the proposed warning and user-generated content." *Herrick*, 306 F.Supp. 3d at 592 (reasoning that "*Internet Brands* is best read as holding that the CDA does not immunize [ ] from a failure to warn claim when the alleged duty to warn arises from something other than user-generated content"—since bad actors contacted Plaintiff offline, did not post any content to the website, and knowledge of the misuse arose from an outside source).

Here, the District Court properly recognized the Putative Class Members' claims are distinct from *Internet Brands* because they are not based on any actual knowledge of the harmful messages sent to the Putative Class Members—but on the policing, editing, and removal of user generated conduct. (ER-74). *See In re Facebook, Inc.*, 2021 WL 2603687, at *10 (CDA barred failure to warn claim clam because "[t]he warnings Plaintiffs seek would only be necessary because of Facebook's allegedly inadequate policing of third party content transmitted via its platforms" and the failure to protect Plaintiffs from third party users on the site). Specifically, the District Court held the Putative Class Members' "accusation here is fundamentally that [Defendants] should have monitored and curbed third-party content" and thus their "theory would require the editing of third-party content, thus treating Defendants as a publisher of content." (ER-12–14) (citing *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.").

Accordingly, the District Court properly found the Putative Class Members' failure to warn claim would require the policing of third-party content to which CDA immunity applies.[5]

[5] The Appellants' negligence claim is premised upon the alleged design defects and failure to warn (same theories at Count 1 and Count 2). (ER-78). Therefore, based

### *c. Appellants' Misrepresentation and False Advertising Claims are Barred by the CDA*

The Putative Class Members' final attempt to plead around Section 230(c)(1) is through their misrepresentation claims. These claims are based on YOLO's alleged representations that it would take actions to implement safety measures, including revealing the identities (ER-42, ER-81) and banning (ER-42) users who send harassing messages (ER-81). The harm caused to the Putative Class Members by each of these allegations is based upon user-generated content and YOLO's screening functions and content moderation. Courts have held that misrepresentation claims based on allegations similar to those alleged by the Putative Class Members, including regarding content moderation and a platform's publishing, screening, and editorial functions, are entitled to CDA immunity.

In *Beckman v. Match.com*, Plaintiff was attacked by an individual she met on the Match.com dating website and later sued Match for negligently misrepresenting the "safety of its website." 2013 WL 2355512 at *6 (D. Nev. 2013). The district court held that such claims are "actually directed at Match.com's publishing, editorial, and/or screening functions—all of which are clearly entitled to immunity under the CDA." *Id*. This Court affirmed the Section 230(c)(1) dismissal, holding that the basis for the negligent-misrepresentation claim was "Match's role as a

---

on the arguments set forth above in sections (3)(a) and (b) and *infra*, the negligence claim is also barred by the CDA.

publisher of third-party information." *Beckman v. Match.com, LLC*, 668 F.App'x 759, 759 (9th Cir. 2016); *see also Opperman v. Path*, 87 F.Supp.3d 1018, 1045 n.12 (N.D. Cal. 2014) (any claims seeking to hold Apple liable for "provid[ing] third-party developers with review guidelines," for Apple's "enforcement of its guidelines," or for Apple's "failure to remove offending apps" from the Apple's App Store were claims that targeted "fundamental publisher activity protected by the CDA"); *Cross v. Facebook, Inc.*, 14 Cal.App.5th 190, 206–07 (2017) (rejecting plaintiff's argument that § 230 did not apply to misrepresentation claims because those claims targeted defendant's failure to remove third party content); *Murphy*, 60 Cal.App.5th at 26-27 (rejecting argument Section 230(c)(1) could not apply because the "only information at issue is Twitter's *own* promises" and not "information provided by another content provider" finding "[c]ourts have routinely rejected a wide variety of civil claims like Murphy's that seek to hold interactive computer services liable for removing or blocking content or suspending or deleting accounts (or failing to do so) on the grounds they are barred by the CDA.") (citations omitted).

In addition, the District Court properly dismissed the misrepresentation/false advertising claims by agreeing with YOLO that the "claims are directed at Defendants' content moderation policies" and thus barred under the CDA. And as discussed in section 2(b), 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. At its core, the claim that YOLO allegedly failed to implement safety features (i.e., ban users who sent harassing messages) is directed at YOLO's screening and content moderation functions. Accordingly, the District Court reasonably found "the accusation here is fundamentally that Defendants should have monitored and curbed third-party content." (ER–11) (citation omitted).

Furthermore, *Omegle.com* is of no help to the Putative Class Members. The harm alleged in *Omegle.com* was a "predictable consequence" of ***an inherently dangerous*** product feature and "a clear example of a claim that simply does not rest on third-party content": it was the product feature that paired a minor with an adult in a private chatroom, and it did so before any content was exchanged between them. *Omegle.com,* 2022 WL 2713721, at *1. The actual content of the posts (i.e., pornographic material of a minor) was not at issue in *Omegle.com* and thus the court held defendant could have satisfied its duty to plaintiff by designing its product differently, for example, by designing a product so that it did not match minors and adults. *Id*. at *4. That is not the case here.

The Putative Class Members' misrepresentation claims are essentially based upon a pop-up in the YOLO app indicating: "YOLO is for positive feedback only. No bullying. If you send harassing messages to our users, your identity will be revealed." (ER-42). This statement is entirely regarding "the general safety of the platform and the enforcement of its guidelines regarding third party content" which

should be dismissed under Section 230 immunity. *See Opperman*, 87 F. Supp. 3d at 1045, n. 12 (stating that app publishing, promulgation of review guidelines, review of apps submitted to the platform, and enforcement of platform's guidelines is "fundamental 'publisher' activity protected by the CDA"); *Gentry*, 99 Cal.App.4th at 833–34 (holding that plaintiffs could not avoid § 230 by attacking the structure of defendant's "safety program"). Indeed, the fact that the Putative Class Members contemplate how "monitoring third-party content" may be "the most practical compliance option to discharge duties to warn and to not to make false and deceptive statements" just further supports how the misrepresentation claims go to YOLO's content moderation policies and is thus a fundamental "publisher" activity protected by the CDA.[6] Opposition Brief p. 45.

Accordingly, in light of the foregoing, YOLO is entitled to CDA immunity for the Putative Class Members' misrepresentation claims.[7]

---

[6] For the remaining unjust enrichment and state-law claims, they are predicated on allegations that YOLO committed false advertising or misrepresentations, or are otherwise coextensive with the negligence or product liability claims. (ER-14, n.5, SER-20–21). Thus, based on the arguments set forth above in sections (3)(a)-(3)(c) for the tort and misrepresentation claims, the unjust enrichment and state-law claims are also barred by the CDA and should be dismissed.

[7] Should the Court consider EPIC's amicus brief, EPIC's position and arguments substantially overlap with those made by the Putative Class Members and add nothing materially different. Accordingly, on the same basis provided in this Answering Brief, the Court should reject EPIC's arguments, find YOLO is entitled to CDA immunity, and affirm, in its entirety, the District Court's order granting YOLO's Motion to Dismiss the FAC with prejudice.

## CONCLUSION

For the foregoing reasons, YOLO respectfully requests that this Court affirm, in its entirety, the District Court's order granting YOLO's Motion to Dismiss the FAC with prejudice.

Dated: November 22, 2023

DENTONS US LLP

*/s/ Nick S. Pujji*
Nick S. Pujji
Carol Yur
Emma Moralyan

*Attorneys for Appellee YOLO Technologies, Inc.*

## STATEMENT OF NO RELATED CASES

Pursuant to Circuit Rule 28-2.6, Appellee YOLO Technologies, Inc. is not aware of any related cases pending before this Court.

Dated: November 22, 2023

DENTONS US LLP

*/s/ Nick S. Pujji*
Nick S. Pujji
Carol Yur
Emma Moralyan

*Attorneys for Appellee YOLO Technologies, Inc.*

## CERTIFICATE OF COMPLIANCE

See attached Form 8.

**UNITED STATES COURT OF APPEALS**
**FOR THE NINTH CIRCUIT**

## Form 8. Certificate of Compliance for Briefs

*Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf*

**9th Cir. Case Number(s)** 23-55134

I am the attorney or self-represented party.

**This brief contains** 13,961 **words,** including _____ words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- (●) complies with the word limit of Cir. R. 32-1.
- ( ) is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ( ) is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ( ) is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ( ) complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
  - [ ] it is a joint brief submitted by separately represented parties.
  - [ ] a party or parties are filing a single brief in response to multiple briefs.
  - [ ] a party or parties are filing a single brief in response to a longer joint brief.
- ( ) complies with the length limit designated by court order dated _____.
- ( ) is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

**Signature** s/ Nick S. Pujji **Date** 11/22/2023

*(use "*s/[typed name]*" to sign electronically-filed documents)*

# ADDENDUM

## ADDENDUM TABLE OF CONTENTS

**47 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) [subparagraph (A)].

(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.

(5) No effect on sex trafficking law.

Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit--

(A) any claim in a civil action brought under section 1595 of title 18, if the conduct underlying the claim constitutes a violation of section 1591 of that title;

(B) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 1591 of title 18; or

(C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of title 18, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

(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.

## CERTIFICATE OF SERVICE

I hereby certify that on November 22, 2023, I electronically filed the foregoing Answering Brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the Court's CM/ECF system.

Dated: November 22, 2023

DENTONS US LLP

*/s/ Nick S. Pujji*
Nick S. Pujji
Carol Yur
Emma Moralyan

*Attorneys for Appellee YOLO Technologies, Inc.*