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.; LIGHTSPACE, INC.,

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

BRIEF FOR PLAINTIFFS-APPELLANTS

JUYOUN HAN
ERIC M. BAUM
ANDREW CLARK
JONATHAN AXEL
EISENBERG & BAUM, LLP
24 Union Square East, Penthouse
New York, New York 10003
(212) 353-8700

Attorneys for Plaintiffs-Appellants

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

PAGE(S)

Cases

Statutes

Rules

PAGE(S)

Other Authorities

INTRODUCTION

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

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

The anonymity-focused design of YOLO's app, offered to teenagers for free, developed a distinct culture of pervasive bullying on the platform. As Carson noted in his text conversation to his friend, the harassing comments were almost

---

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

exclusively sent through YOLO, and not on other apps. YOLO's anonymity feature follows a long lineage of similarly designed products, each of which foster drama, hate, and bullying, with sometimes fatal consequences to users. The Complaint outlined these anonymous applications and the teen user-victims throughout the years who took their own lives as a result.

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

Adding to the recipe for chaos, YOLO then lied to young consumers that it had a safety switch —an identity reveal— which turned out to be completely

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

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

Decency Act, that was designed to disincentivize the exact kind of conduct seen here.

JURISDICTIONAL STATEMENT

This Court has jurisdiction under 28 U.S.C. §1291 as an appeal from a final decision of the District Court dismissing all claims with prejudice dated January 10, 2023. ER-2. Plaintiffs timely appealed on February 9, 2023. EC-106; Fed. R. App. P. 4(a)(1)(A).

FACTUAL BACKGROUND

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

"YOLO" is an acronym for the phrase "You Only Live Once," and name of the mobile phone application ("app") developed and operated by the Defendant-Appellee, Yolo Technologies Inc. (hereinafter, YOLO). *See* ER-17 (Amended Complaint ("AC") ¶ 1). Within a week of YOLO's launch in 2019, it became the top downloaded app in America and a "teen hit," and within months the app had 10 million active users. ER-18 (AC ¶ 4).

YOLO was marketed for "teens" in app stores, inviting minors to integrate an anonymous messaging tool to the popular Snapchat platform. *See* ER-39, 45-46 (AC ¶¶ 60, 74-76). YOLO was intentionally designed with one defining feature: enabling users hide their identities when commenting on a Snapchat post (a popular social media platform whose developer, Snap, Inc., was dismissed from

this case through a settlement). By using YOLO's product: (1) Snapchat users can create and publish a story (called "posting") on their account (non-anonymous) and include a question for friends or audience to answer using YOLO's anonymity tool (*see* ER-51 (AC ¶¶ 98 & 99)); (2) when another Snapchat user comments on a post, the commenter's username is sent to the Snapchat user anonymously (*see* ER-38, 45 (*see* AC ¶¶ 56 & 73)); and (3) the anonymous commenter can voluntarily reveal themselves by "swiping up," but the receiver of the anonymous message cannot require the anonymous commenter to do so. ER-26-27, 38, 50 (*see* AC ¶¶ 26, 56 & 96). As a one-sided invisibility cloak, this YOLO feature protects users who wish to withhold their identity while keeping the message recipient in the dark – a perfect tool for cyberbullying.

It was well-known that bullying and harassment would manifest from anonymous messaging apps because this long lineage of anonymous apps that YOLO followed were already associated with teen suicides. ER-32-35 (AC ¶¶ 40-48). As Carson noted in his text conversation to his friend, the harassing comments would particularly come through YOLO, not on other apps. *See* ER-51 (AC ¶97).

YOLO was well-aware of this, but it made bold promises for safety on its app to users, which turned out to be a lie. When a user first opens YOLO after downloading it from the Apple or Google app stores, a pop-up notice fills the screen and tells each prospective user: "YOLO has no tolerance for objectionable

content or abusive users. You'll be banned for any inappropriate usage." The Complaint alleges that Carson and all Plaintiffs-Appellants saw and relied upon this statement to their detriment. *See* ER-55, 57 (AC ¶¶ 123, 134). However, YOLO did not have any mechanism in place for investigating or responding to reports made by its users or their guardians. S*ee* ER-38, 43 (AC ¶ 57 & 70). In fact, according to YOLO's own sworn declaration in this case, fewer than 10 employees were accountable for YOLO's 10 million daily active users as of 2021. *See* ER-38-39 (AC ¶ 58). YOLO knew that it could not possibly provide meaningful safeguards to so many active users. According to Customer Reviews, YOLO repeatedly ignored reports of dangerous levels of harassing and bullying behavior on YOLO. *See* ER-43 (AC ¶¶ 70-71) (quoting YOLO customer review: "(d) "My daughter has been getting bullied on this app and we report/block, and this bully keeps on going and it's about suicide! . . . If someone truly reports someone this nasty on the app, it should be dealt with instantly! (e) . . . At a time when suicide is the number 1 killer of teens in America, we definitely don't need apps like this where bullied haters can hide behind a screen (g) . . . it's teaching our youth that it's okay to hide behind a screen and bully. So if someone want to say(sic) something nice, they should say it to them directly, not through an anonymous messaging app where people are constantly getting hurt and bullied.").

Lead Plaintiff-Appellee Carson Bride

On June 23, 2020, the Bride family, of Oregon, was struck by an unthinkable tragedy. *See* ER-20 (AC ¶ 10). 16-year-old Carson Bride took his own life after suffering months of cyberbullying on YOLO and LMK. *Id*. These messages included physical threats, obscene sexual messages and propositions, and other humiliating comments. *See* ER-49 (AC ¶ 90-91). Carson's efforts to find his tormentors on the anonymous app were futile: he asked the commenters to voluntarily S/U (swipe up) but the harassers remained hidden; he asked other classmates about the identity of commenters, but they had no way of knowing. *See* ER-50-51 (AC ¶ 96-98). On the night of his death, Carson's web search history shows that he was searching how to reveal YOLO usernames. *See* ER-51 (AC ¶ 100).

Two weeks after Carson's death, Carson's grieving parents Kristin and Tom Bride contacted YOLO on their "Contact Us" form and Customer Support page, writing about the cyberbullying that led to Carson's death and asking for the harassing users' identities to be revealed. *See* ER-52-54 (AC ¶¶ 105-117). Despite YOLO's promise to ban and reveal the identities of harassing and bullying users, YOLO did not respond. *Id*. Carson's parents then attempted to make contact through YOLO's law enforcement email address, but the message would not even

transmit. *See id*. Through a professional contact, they then reached out personally to YOLO's founder, Gregory Henrion, but still received no response. *Id*.

On May 10, 2021, Carson's mother Kristin, along with the national non-profit organization Tyler Clementi Foundation, filed this lawsuit against YOLO and two other defendants in the case. ER-16. Within 48 hours of filing the lawsuit, Snap Inc. ("Snap") suspended YOLO and LMK from Snapchat. ER-20-21 (AC ¶ 12). And on March 17, 2022, Snap announced that it would fully ban anonymous messaging apps like YOLO and LMK from its platform. *Id*. As Snap explained, "we believe some users" of "anonymous integrations" like YOLO and LMK "might be more prone to engage in harmful behavior — such as bullying or harassment — if they have the shroud of anonymity." *Id*.

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

The Tyler Clementi Foundation brings claims as an organizational plaintiff on behalf of itself and its associated members (e.g., Youth Ambassadors). ER-89 (AC ¶ 268). The Foundation's mission and activities focus on educating parents, schools, and children about preventing cyberbullying and providing effective interventions in cyberbullying scenarios. The Foundation alleged that it diverted research and investigation resources specifically into the harms of anonymous apps due to their known dangers. ER-61-62 (AC ¶ 156). And because YOLO frustrated

the organization's purpose of preventing cyberbullying, the Foundation and its associated members alleged that they were injured. *See* ER-31 (AC ¶ 36).

A.K., A.C., and A.O. joined the lawsuit and their claims were included in the Amended Complaint. A.K. is a minor child who used YOLO and was persistently harassed by those sending vicious anonymous messages. *See* ER-55-56 (AC ¶¶ 122-27). The anonymous users encouraged her to commit suicide, sent death threats, and made body shaming remarks. *Id*. Relying on YOLO's statement that it would reveal harassers' identities, A.K. sent requests to YOLO to reveal her bullies' identities but YOLO ignored her request. *Id*.

A.C. was only 13 years old when she used YOLO and suffered from harassing messages. The anonymous messages encouraged her to commit suicide while she was grieving the recent death of her brother, and included body-shaming comments. *See* ER-56-58 (AC ¶¶ 129-140). A.C.'s frustrations grew as she could not find a way to discover the identities of the vicious YOLO users who were protected by YOLO's anonymity product. *Id*.

A.O. is a minor child who used YOLO and was harmed by harassing and bullying messages. *See* ER-58-59 (AC ¶¶ 141-48). The messages she received through YOLO included being called offensive names such as a "whore," sexual solicitation, and body-shaming remarks. *Id*. A.O. was unable to discover the

identities of the senders of those messages because they were protected by YOLO's anonymity product. *Id*.

Complaint

Plaintiffs-Appellants brought a national class action representing a class and subclasses of individuals who used YOLO and were similarly harmed. In the Complaint, Plaintiffs-Appellants asserted (1) strict product liability based on a design defect; (2) strict product liability based on a failure to warn; (3) negligence; (4) fraudulent misrepresentation; (5) negligent misrepresentation; (6) unjust enrichment; (7) violation of the Oregon Unlawful Trade Practices Act; (7) violation of the New York General Business Law § 349; (8) violation of the New York General Business Law § 350; (9) violation of the Colorado Consumer Protection Act; (10) violation of the Pennsylvania Unfair Trade Practices Law; (11) violation of the Minnesota False Statement in Advertising Act; and (12) violation of California Business and Professions Code §§ 17200 & 17500. *See* ER-23-29 (AC ¶¶ 20-30, 178-322).

Throughout this brief, the strict liability, negligence, and state statutory claims that relate to YOLO's inherently dangerous and defectively designed product are referred as "Products Liability Claims"; the claims related to YOLO's failure to warn users of the danger of their products are referred to as "Failure to

Warn claims"; and the claims asserting that YOLO made fraudulent misrepresentations and false advertising are referred to as the "Misrepresentation and False Advertising Claims."

The Complaint made clear that it does not "seek to hold Yolo or Lightspace liable as the publisher or speaker of the content provided by third parties within the meaning of Section 230. Instead, the plaintiffs seek to hold the defendants liable for their own conduct, namely their negligent design of products that would cause foreseeable harm that outweighs the utility of their products, their own failure to warn of the danger of their products, and their own misrepresentations about the specific steps they would take to stop harassment and bullying of users." ER-22 (AC ¶ 17).

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

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

ER-22-23 (AC ¶ 18). The Complaint specified that YOLO's anonymity product itself inherently causes harm and psychological anxiety independent of the content of the messages sent using the product. For example, Carson's continued and painstaking efforts to investigate his harassers' identity until moments before his death demonstrates the tormenting anxiety and pressure that YOLO's anonymity feature imposed on him. *See* ER-51 (AC ¶ 97). Anonymity hinders victims from appropriately handling the content of messages because it deprives them of any means of confronting the perpetrators or assessing the possible reasons for those messages, and this leaves a sense of unresolved anger and harm especially in developing teenagers that makes it impossible for guardians, schools, or law enforcement to intervene. *See* ER-38 (AC ¶ 56).

Moreover, YOLO's false statement creates a new type of harm that is separate from the third-party messages. This includes the level of stress and frustration that was experienced by Carson as he was searching online for means to reveal his YOLO bullies on the night prior to his death. *See* ER-50 (AC ¶ 94). Similarly, A.K., A.O., and A.C. were harmed when they all relied upon YOLO's statement that harassing users will be unmasked, and later their requests to reveal the identities of harassers were ignored. *See* ER-56-59 (AC ¶¶ 122-48).

District Court's Decision

In a decision dated January 10, 2023, the District Court held that "Section 230 immunizes Defendant[-Appellee] from Plaintiffs' claims in their entirety" and dismissed the Complaint with prejudice. ER-14. The District Court reasoned that while Plaintiffs-Appellants' claims "frame user anonymity as a defective design feature of Defendants' applications, Plaintiffs fundamentally seek to hold Defendants liable based on content published by anonymous third parties on their applications. Accordingly, the court finds Plaintiff's theories of liability treat Defendants as a "publisher" within the meaning of Section 230." ER-8. The lower court further held that YOLO's decision to allow or prevent users from using anonymity tools are "decisions about the structure and operation of a website are content-based decisions" under Section 230." ER-9. The District Court added that the claims here are not distinguishable from "*Dyroff* given the Ninth Circuit ultimately concluded that the defendant was entitled to immunity under the plain terms of Section 230 and our case law as a publisher of third-party content because the plaintiff could not and did not plead that the defendant required users to post specific content, made suggestions regarding the content of potential user posts, or contributed to making unlawful or objectionable user posts." ER-9 (internal citations and quotations omitted).

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

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

ER-10. With regard to the Misrepresentation and False Advertising Claims, the District Court held that "those claims are still predicated on content developed by those third parties. Had those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable." ER-11. Dismissing the Failure to Warn Claims, the lower court found them barred by the CDA because "Plaintiffs' theory would require the editing of third-party content, thus treating Defendants as a publisher of content. Accordingly, *Internet Brands* is inapposite on this issue." ER-13.

PROCEDURAL HISTORY

Representing Carson Bride's estate, Carson's mother Kristin Bride brought the initial Complaint on May 10, 2021, against Defendant-Appellant YOLO and former Defendants Snap, Inc., and Lightspace Inc. in the Northern District of

California. ER-112 (Dkt. 1.) The venue was transferred to the Central District of California on August 18, 2021. ER-117-18 (Dkts. 49-50 & 53.). Plaintiff filed the First Amended Complaint on June 27, 2022. ER-124 (Dkt. 113). YOLO submitted a motion to dismiss on October 6, 2022 ER-127 (Dkt. 127). The lower court heard oral argument on January 5, 2023. ER-127 (Dkt. 141). A decision granting the motion to dismiss with prejudice was issued on January 10, 2023. ER-127 (Dkt. 142). Plaintiffs-Appellants timely appealed on February 9, 2023. ER-127 (Dkt. 143). Claims were withdrawn and dismissed against Defendant-Appellant Lightspace on August 11, 2023. *See* Unopposed Mot. To Dismiss Party, Dkt. 22.

STATEMENT OF THE ISSUES

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

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

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

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

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

STANDARD OF REVIEW

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

SUMMARY OF ARGUMENTS

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

children from harmful contents and encourage removal of harmful contents. The District Court's decision contravenes the plain text of the statute and all of the stated policy goals therein.

Moreover, the District Court's dismissal of the Plaintiffs-Appellants' complaint is unsupported by this Court's precedents. In *Barnes v. Yahoo!, Inc.*, this Court created a three-pronged test for determining whether an internet company may be exempt from liability under Section 230. 570 F.3d 1096, 1100 (9th Cir. 2009). Under this test, immunity from liability exists for "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider." *Id.* at 1100-01.

Here, the first prong is undisputedly met, because Defendant-Appellee is the developer of a mobile application that allows users to communicate with one another. Regarding the second prong, however, the District Court erred by foregoing an analysis of whether the duty in each of Plaintiffs-Appellants' claims arise from the internet company's role as a publisher or a product manufacturer, instead adopting a "but-for" test that has already been rejected by this Court. As for the third prong, the District Court further erred by ignoring facts alleging that Defendant-Appellee was responsible as an information content provider, and failed to draw all factual inferences in Plaintiffs-Appellants' favor when it found that

YOLO was a content-neutral tool that did not encourage any unlawful or objectionable content. The District Court further erred by dismissing Plaintiffs-Appellants' failure to warn and misrepresentation/false advertising claims, which are solely based on Defendants' own conduct and statements.

ARGUMENT

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

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

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

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

> "(1) Treatment of publisher or speaker
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

47 U.S.C. § 230 (c)(1).

The purposeful use of the phrase "treated as the publisher or speaker," by its plain meaning, "cuts off liability only when a plaintiff's claim faults the defendant for information provided by third parties." *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1093 (9th Cir. 2021) (emphasis added) (citing 47 U.S.C. § 230 (c)(1)).

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

to be held liable under publisher-based claims in the course of removing objectionable content.

Aligned with this reading, the Seventh Circuit clarified that "§ 230(c)(1) is not a comprehensive grant of immunity for third-party content. Instead, that subsection precludes liability only where the success of the underlying claims requires the defendant to be considered a publisher or speaker of that content. But § 230(c)(1) may not necessarily preclude liability if the underlying claims identify the interactive computer service's own content as objectionable." *Webber v. Armslist LLC*, 70 F.4th 945, 957 (7th Cir. 2023) (emphasis added).

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

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

The purpose of the CDA is written in its title: "Protection for Good Samaritan Blocking and Screening of Offensive Material." 47 U.S.C. § 230. It extends to "any action voluntarily taken in good faith to restrict access to or

availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." 47 U.S.C. § 230(c)(2)(A) (emphasis added).

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

> (1) to promote the continued development of the Internet . . . (2) to preserve the vibrant and competitive free market that presently exists for the Internet. . . (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material . . ."

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

Allowing internet companies that host third-party content to be free from liability, regardless of whether they are making good-faith efforts to prevent harm as "Good Samaritans," contradicts Congress's stated aim in enacting the CDA. Here, the Complaint alleged that YOLO designed an app with anonymity

features—knowing these features would induce harassing and harmful messages—and assured consumers by representing that it had safety measures in place, without actually implementing them. *See* ER-65 (AC ¶ 65). YOLO's conduct is completely inconsistent with that of a "Good Samaritan." YOLO drew in vulnerable minor users with its attractive anonymity feature, gave a false sense of security to guardians, bystanders, and users with empty promises and ineffective guardrails, and now attempts to exploit the CDA shield.

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

Unless reversed, this precedent will permit companies to develop and profit from all kinds of dangerous and deceptive products. Currently, too many internet companies profit from feeding harmful and egregious content to young users, from

unrealistic beauty standards to the sale of child pornography, sale of illicit and fatal drugs, and promotion of gun violence and terrorism. Left to their own devices, social media apps will be designed to increase the publication and consumption of addictive, salacious, and dangerous content driven by short term market incentives for companies to "race to the bottom." Technology already exists that would allow a suite of unthinkably horrifying conduct if companies were unrestrained in how they implement it. Imagine, for example, deepfake and generative artificial intelligence tools used by children on social media enabling creation of images that depict violence, nudity, and other harmful contents just by typing in a prompt; rigged location sharing technology or hacking tools that are used over social media to bypass safety guidelines set by law enforcement and guardians, combined with lucrative ingredients like anonymity, lack of age-verification, and data privacy intrusions. Should the District Court's precedent stand, individuals and companies would use those technologies to exploit social unrest, mistrust, and even violence for short-term profit, all while enjoying broad protection under the CDA. Ultimately, young users, parents, and students alike who are victims of these unchecked technologies are not only lied to but are left without any recourse when they are harmed. Therefore, based on the plain text of the statute and the policy purposes expressed by Congress, this Court must reverse the District Court's decision and allow Plaintiffs-Appellants' claims to proceed.

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

The District Court erred in deciding that the second prong of *Barnes* was met by adopting and applying a "but-for" publication test – that CDA immunity applies if a cause of action would not be cognizable "but-for" content from a third party. *See* ER-11 ("Had those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable.").

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

Section 230 immunity did not apply to the plaintiff's failure to warn claims, and in its reasoning, expressly rejected a "but-for" test:

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

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

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

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

In *Barnes v. Yahoo!, Inc.,* the plaintiff brought negligence and promissory estoppel claims against Yahoo for failing to remove her ex-boyfriend's posts

containing nude photographs of her. This Court's decision parsed the negligence from the promissory estoppel claims by examining whether the duty of Yahoo to remove third-party content derives from the internet company's role as a publisher or a party to a contract. This Court found that in the negligence claims, the duty arose from Yahoo's role as a publisher, but in the promissory estoppel claim, the duty arose from Yahoo's contractual obligation to remove the injurious content. *Id.* at 1107-07 ("Barnes does not seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promisor who has breached."). This Court further explained that "[c]ontract liability here would come not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication." *Id.* at 1107 (emphasis added).

In this case, the products liability, negligence, and state consumer protection claims seek to hold YOLO liable for failing to take actions to increase the safety of its consumers from the harms of cyberbullying, such as removing offensive users from its platform or revealing their identities. Like *Barnes*, this duty does not derive from YOLO's publishing conduct, but from YOLO's role as a developer, seller, and advertiser of its anonymous messaging product, where it unequivocally expressed that it would remove or reveal the individuals who harass or bully others on its platform. Applying *Barnes* to this case, even if YOLO's removal or

revealing identities of individuals happens to coincide with YOLO's duty as a publisher, this does not activate CDA immunity because Plaintiffs-Appellants' claims rely upon a duty – the duty to make reasonably safe products – that is separate from YOLO's publisher duty. *See id*.

Instead, the lower court departed from *Barnes* by ruling that CDA immunity applies because Plaintiffs-Appellants' claims require YOLO to monitor third-party content by ensuring that each post can be traceable to the sender:

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

ER-10. The District Court's reasoning above failed to even attempt to identify the duty in each of Plaintiffs-Appellants' claims, despite this Court's holding in *HomeAway.com* 918 F.3d 676 (9th Cir. 2018). In *HomeAway*, the city of Santa Monica passed an ordinance requiring internet platforms that host rental properties to ensure that the properties listed are licensed and listed on the City's registry before completing any booking transactions. The hosting platform, HomeAway argued that CDA granted immunity from suit under the ordinance because the property listings published on its platform were third party content.

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

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

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

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

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

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

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

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

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

ER-22 (AC¶ 18).

Other circuit courts have joined in rejecting a "but-for" test, instead opting to examine the duty underlying each specific claim alleged for purposes of CDA immunity. For example, in *Henderson v. Source For Pub. Data, L.P.*, 53 F.4th 110, 122 (4th Cir. 2022), the court reasoned that the CDA does not bar claims brought under the Fair Credit Reporting Act against companies that publish consumer credit information online:

> Most of what Public Data allegedly does, after all, is publish things on the internet. That means that publishing information is one but-for cause of these FCRA claims against Public Data. If Public Data is a

> "consumer reporting agency" subject to FCRA liability, it is one because it is the publisher or speaker of consumer report information. Yet that alone is not sufficient, as we do not apply a but-for test. See Erie Ins., 925 F.3d at 139-140; HomeAway.com, 918 F.3d at 682. We must instead examine each specific claim.

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

In this case, the District Court incorrectly concluded that Plaintiffs-Appellants' claim was reduced to publisher liability because it would require YOLO to "monitor third-party content . . . in the form of requiring Defendants to ensure that each user's post on their applications is traceable to a specifically identifiable person." ER-10. This conclusion contains a logical error: a product liability claim does not always require a duty to monitor, and a duty to monitor claims can stem from non-publisher liability. As held by this Court in *Lemmon,* "The duty to design a reasonably safe product is fully independent of [a defendant's] role in monitoring or publishing third party content." 995 F. 3d at 1092. That a defendant allows "its users to transmit user-generated content to one another does not detract from the fact that [a plaintiff] seek[s] to hold [the defendant] liable for its role in violating its distinct duty to design a reasonably safe product." *Id*. This Court in *Barnes* also explained that the CDA does not bar promissory estoppel claims where a duty to monitor is generated by contract liability where an internet company is a party to a contract. *Barnes*, 570 F.3d at 1107 ("[c]ontract liability here would come not from Yahoo's publishing conduct,

but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication.").

The District Court's opinion also forces factual inferences not contemplated or asserted in the pleadings when it noted that the Plaintiffs-Appellants' claim requires monitoring the form of ensuring that each user's post is traceable to an identifiable person. *See* ER-10. As alleged in the Amended Complaint, YOLO users are already traceable and identifiable, because they can either remove their anonymity by voluntarily "swiping up" or, as YOLO advertised, by YOLO removing the user's anonymity mode. ER-26-27 (AC ¶ 26). Hence, YOLO could have complied with its duty under products liability law by, among other means, simply allowing receivers of anonymous messages to remove their sender's anonymity and reveal their identity. In its opinion, the District Court did not accept the Complaint's factual allegations as true and draw all factual inferences in Plaintiffs-Appellants' favor – which it was required to do at the motion to dismiss stage. *See* Fed. R. Civ. P. 12; *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1090 (9th Cir. 2021) (holding that a "complaint will survive at this stage if it states 'a plausible claim for relief'").

Therefore, the District Court's adoption of the "but-for" rule in reviewing the second prong of *Barnes* is already rejected by this Court, and its failure to parse out the duty underlying each of Plaintiffs-Appellants' claims, led to an erroneous

conclusion. Its reasoning conflicted with binding precedent of this Circuit, and its holding should therefore be reversed.

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

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

This Court has held that a website can be liable as an information content provider if they "create or develop" content "by making a material contribution to

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

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

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

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

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

an essay answer. *Id.* at 1124. This Court noted that the defendant company was not responsible "even in part, for associating certain multiple-choice responses with a set of physical characteristics, a group of essay answers, and a photograph." *Id*. Under those circumstances, the court concluded that the dating site could not be considered an "information content provider." *Id.*

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

In *Gonzalez v. Google LLC*, families of deceased victims of an ISIS terrorist attack brought claims against Google under the Anti-Terrorism Act (ATA), 18 U.S.C.S. § 2333, alleging that Google was directly and secondarily liable for allowing ISIS to post content communicating the group's support for terrorism by

publishing, recommending, and providing such content on the social media platforms. 2 F.4th 871 (9th Cir. 2021), *rev'd on other grounds*, 598 U.S. __ (2023). There, this Court reviewed the factual allegations regarding Google's algorithms to determine whether Google prompted users to post unlawful content. This Court found that the algorithm behind Google's search engine – which allegedly selects particular content for a user based on the user's own inputs – would be considered a content-neutral tool because it does not "provide any encouragement to perform illegal searches or to publish illegal content." *Id.* at 896.

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

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

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

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

- ER-17-18 (AC ¶ 3): anonymous online communications pose a significant danger to minors, including by increasing the risk of bullying and other antinormative behavior and amplifying the negative feelings of victims . . . Prior anonymous apps were "vulnerable to being used to spread hate speech and bullying.

- ER-43-44 (AC ¶ 71): (YOLO customer review) (e) . . .At a time when suicide is the number 1 killer of teens in America, we definitely don't need apps like this where bullied haters can hide behind a screen . . . (h) . . . it's teaching our youth that it's okay to hide behind a screen and bully. So if someone want to say something nice, they should say it to them directly, not through an anonymous messaging app where people are constantly getting hurt and bullied.

- ER-51 (AC ¶ 97): Do you know who is sending me all these sus(picious) YOLOs. Whenever I do one I only get people either trying to catfish me or bait me into saying dumb (things) or whatever . . . I guess I understand like a bit of sus(picious) shit every once in a while but it [is] my entire inbox of YOLO's.

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

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

ER-9 (quoting *Dyroff*, 934 F.3d at1099). Unlike the website Experience Project in *Dyroff*, where every user had a registered name attached to their posts, and every user remained pseudonymous (*id*. at 1100), YOLO was designed to give a one-

sided privilege to keep the message sender anonymous, while the message receiver was identifiable. *See* ER-26, 38, 50 (AC ¶¶ 26, 56 & 96). This made targeted bullying inevitable, especially when unassuming teens would rely on YOLO's self-stated promise to reveal harassers' identities while using the app. The District Court further cited to other decisions where anonymity was a common component of a website but was designed and marketed with significant differences from YOLO, such as adult websites that "g[a]ve an option to anonymize email addresses." ER-9 (*citing Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116, 1124 (N.D. Cal. 2016) and *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 20 (1st Cir. 2016)).

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

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

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

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

Nothing in the text, purpose, legislative history, or courts' interpretation of the CDA allows internet companies to avoid liability for harms that derive from their own conduct and speech. The second prong of the test under *Barnes*, based on the text of the statute, is that the CDA would cut off liability where an internet company is treated as the "publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230 (c)(1); *Barnes v. Yahoo!,*

Inc., 570 F.3d 1096, 1100 (9th Cir. 2009); *see also Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1093 (9th Cir. 2021).

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

The District Court's decision to dismiss the Plaintiffs-Appellants' failure to warn and misrepresentation/false advertising claims run counter to this Court's precedents. In *Doe v. Internet Brands*, 824 F.3d 846, 853 (9th Cir. 2016), this Court made clear that a plaintiff's failure to warn claims were not barred by the CDA where they are not based on any content posted on the website. Because the duty under the plaintiff's failure to warn claims did not require any action regarding third-party content posted on its site, the claims did not treat the defendant as a publisher or speaker of information. *See id.; see also A.M. v.*

Omegle.com, LLC, 614 F. Supp. 3d 814, 820 (D. Or. 2022) (holding that the defendant failed to warn minor users about adult predators on the website, and that the website could have discharged the duty without having to "alter the content posted by its users—it would only have to change its design and warnings.").

Here, in dismissing Plaintiffs-Appellants' failure to warn claims, the District Court merely stated: "Plaintiffs' theory would require the editing of third-party content, thus treating Defendants as a publisher of content. Accordingly, *Internet Brands* is inapposite on this issue." *See* ER-12-13. The District Court's finding has no basis in the Amended Complaint, which alleged the contrary: "YOLO . . . could have complied with their duty to warn users (and users' parents and guardians) of the danger of anonymous messaging without monitoring or changing the content of users' messages." ER-22-23 (AC ¶ 18). Furthermore, the duty to warn only requires that YOLO create a proper warning about the proliferation of harassment and bullying, which they knew about through reports from consumers, or even provide individualized warnings. ER-43-44 (AC ¶ 71). The District Court's decision is void of explanation as to why it inferred that the duty would require editing of any third-party content.

The District Court's dismissal of the misrepresentation/false advertising claim is similarly flawed. It reasoned that Plaintiffs-Appellants' misrepresentation and false advertising claims are still predicated on third-party content because

"[h]ad those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable. . . . In sum, the accusation here is fundamentally that Defendants should have monitored and curbed third-party content." ER-11.

The District Court's logic fails for several reasons. First, the duty not to make false statement depends on YOLO's own affirmative statement to its users, in a conspicuous pop-up message: "YOLO is for positive feedback only. No bullying. If you send harassing messages to our users, your identity will be revealed." ER-41 (AC ¶ 65). The underlying duty not to make false statements is based on the factual allegation that Plaintiffs-Appellees read and relied upon this statement when they began using YOLO. *Id*. Hence, liability for misrepresentation/false advertising depends on YOLO's own promise to stop and reveal bullying and harassing users, not on YOLO's publishing conduct. Such conclusion conforms with this Court's precedent in *Barnes v. Yahoo!, Inc.,* where this court found that the CDA did not exempt Yahoo for liability under promissory estoppel claims because the duty arose from Yahoo's contractual obligation to remove the injurious content. *Barnes*, 570 F.3d at 1105-07; *see also id.* at 1107 ("[c]ontract liability here would come not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication.") (emphasis added).

Second, as discussed above in Section B, *supra* at 24, the District Court's reasoning contains exactly the kind of but-for standard that was outright rejected by Ninth Circuit precedent. *See* ER-11 ("[had] those third-party users refrained from posting harmful content, Plaintiffs' claims that Defendants falsely advertised and misrepresented their applications' safety would not be cognizable. . ."). This type of reasoning would cause absurd results. For instance, if an internet company advertised that its messaging product charges users one dollar for each message sent, when in fact it charged two dollars per message, applying the District Court's reasoning, such false advertisements would still receive protection under the CDA because the harms would not have happened but-for the users' posting of messages. The District Court's conclusion effectively creates a "buyer beware" scenario without actually requiring the seller to warn the buyer, like in this case, allowing the seller to willfully lie to the buyer.

Third, the District Court erred in its conclusory finding that "[t]he accusation here is fundamentally that [Defendants] should have monitored and curbed third-party content." ER-11. YOLO could have discharged its duty not to make false statements to consumers simply by refraining from making false statements to consumers. *A.M. v. Omegle.com, LLC*, 614 F. Supp. 3d 814, 819 (D. Or. 2022) (holding that CDA did not apply to the design defect and failure to warn claims because the internet company could have satisfied its duty simply by designing the

product differently and changing its warnings, without any need to review, edit, or withdraw third-party content). YOLO could have truthfully stated that it lacked the capability or capacity to track harassers and bullies on its app, thereby putting minor users and their guardians on notice and allowing users to make informed decisions about either avoiding the app or implementing their own safety measures. *See* ER-22-23 (AC ¶ 18). ("Yolo . . . could have complied with their duties under the common law and state statutory law not to make false, deceptive, or misleading statements simply by accurately describing their own products, services, and business practices, or by not making such statements at all."). However, by notifying users that it would reveal harassers and bullies, YOLO misled its users.

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

under these circumstances would risk exempting them from most local regulations . . .").

Therefore, this Court should reverse the District Court's decision to dismiss Plaintiffs-Appellants' failure to warn claims and misrepresentation/false advertising claims, which are solely based on Defendant-Appellee's own conduct and statements, not of any third-party users.

CONCLUSION

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

Dated: August 11, 2023

Respectfully submitted,

By: /s/ Juyoun Han

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

Attorneys for Plaintiffs-Appellants

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitations of Circuit Rule 32-1 and Fed. R. App. P. 32(a)(7)(B)(i) because it contains 10,848 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared using a proportionally spaced typeface using Microsoft Word 2010 in Times New Roman 14-point font.

Dated: August 11, 2023

By: /s/ Juyoun Han

CERTIFICATE OF SERVICE

I, Juyoun Han, a member of the Bar of this Court, hereby certify that on August 11, 2023 I caused to be electronically filed with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system the following document:

APPELLANTS' OPENING BRIEF

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: August 11, 2023

By: /s/ Juyoun Han