2022 WL 4009918
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

IN RE: APPLE INC. APP STORE SIMULATED CASINO-STYLE GAMES LITIGATION
IN RE: GOOGLE PLAY STORE SIMULATED CASINO-STYLE GAMES LITIGATION
IN RE: FACEBOOK SIMULATED CASINO-STYLE GAMES LITIGATION

Case No. 5:21-md-02985-EJD, Case No. 5:21-md-03001-EJD, Case No. 5:21-cv-02777-EJD
|
Filed 09/02/2022

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTION TO DISMISS PURSUANT TO SECTION 230 OF THE COMMUNICATIONS DECENY ACT; *SUA SPONTE* CERTIFYING ORDER FOR INTERLOCUTORY APPEAL

EDWARD J. DAVILA United States District Judge

***1** In this putative class action, Plaintiffs allege that Defendants Apple, Google, and Facebook violate various state consumer protection laws by distributing game applications ("apps") that operate as social casinos and thus permit illegal gambling. Defendants separately move to dismiss the complaints against them, arguing that they are immune from suit under Section 230 of the Communications Decency Act ("CDA"). Having considered the Parties' written submissions as well as the oral arguments of counsel presented at the hearing on August 4, 2022, the Court **GRANTS IN PART AND DENIES IN PART** Defendants' respective motions to dismiss.

I. BACKGROUND

Over the last decade, large social media companies and technology developers have turned their focus on developing applications or "apps." As relevant in this case, slot machine companies have partnered with technology companies to develop "social casino applications." Plaintiffs' Master Complaint [1] ("Compl.") ¶ 1, Dkt. No. 73. Social casinos are playable "apps" that can be accessed via smartphones, tablets, and internet browsers. These virtual casinos attempt to recreate an "authentic Vegas-style" slot-machine, gambling experience. Compl. ¶ 2.

The simulated social casino apps are designed to look like traditional casino games, such as slot machines, bingo, or craps. This seemingly makes social casinos apps addictive in the same way as "in-person" gambling. Compl. ¶¶ 3, 4. Indeed, the social casinos apps function much like in-person gambling. Users purchase virtual "chips" in exchange for real money. Compl. ¶ 3. Users then gamble those chips at slot machines games in hopes of winning "still more chips to keep gambling." Compl. ¶ 3. For example, in "DoubleDown Casino," players purchase "chip packages" costing up to $499.99, and then use those chips to play. Compl. ¶ 3. However, social casinos do not allow players to cash out their chips. Compl. ¶ 3. Instead, both purchased and "won" chips can only be used for more slot machine "spinning." Compl. ¶ 3. This makes the social casino apps "extraordinarily profitable and highly addictive." Compl. ¶ 4. One important distinction, however, is that social casino developers have access to big data, which allows them to identify, target, and exploit consumers prone to addictive behaviors. Compl. ¶ 4.

Plaintiffs allege that these social casino apps do not, and cannot, operate and profit at such a high level from these illegal games on their own. *See* Compl. ¶ 5 ("Their business of targeting, retaining, and collecting losses from addicted gamblers is inextricably entwined with the Platforms."). The Platforms "retain full control over allowing social casinos into their stores, and their distribution and promotion therein," and "share directly in a substantial portion of the gamblers' losses, which are collected and controlled by the Platforms themselves." Compl. ¶ 5; *see also* Compl. ¶ 6 ("Because the Platforms are the centers

for distribution and payment, social casinos gain a critical partner to retain high-spending users and collect player data, a trustworthy marketplace to conduct payment transactions, and the technological means to update their apps with targeted new content designed to keep addicted players spending money."). Importantly, each complaint alleges that Apple, Facebook, and Google conspired with the social casino app developers to participate in a pattern of racketeering activity in violation of the Racketeer Influenced and Corrupt Organizations Act ("RICO"). Compl. ¶¶ 16, 17, 489–521; Google Complaint ¶¶ 16, 17, 505–37, Dkt. No. 52; Facebook Complaint ¶¶ 16, 17, 467–99, Dkt. No. 80.

A. Offering, Categorizing, and Promoting of the Social Casino Apps

***2** Each year, consumers buy billions of dollars of online casino chips from the Platforms. The Platforms help the social casino app developers target consumers to maximize revenue. Compl. ¶ 87. "For instance, [Defendant] Apple provides marketing guidance, tools, promotional offers, and more to app developers (like the developers of the Illegal Slots) to help drive users' discovery of apps and in-app purchases." Compl. ¶ 87; *see also* Google Complaint ¶ 85; Facebook Complaint ¶¶ 71, 171 ("Underlying our paid marketing efforts are our *data analytics* that allow us to estimate the expected value of a player and adjust our user acquisition spend to a targeted payback period." (emphasis added)). Defendant Apple selects apps to "feature" within its App Store, which "increases app installs." Compl. ¶ 88. Google "offers App Campaigns to promote apps on Google Search, YouTube, Google Play, and more." Google Complaint ¶ 85. Likewise, Facebook uses tools like "targeted ads" and "in-game rewards" to encourage new users to play social casinos. Facebook Complaint ¶ 80.

Defendant Apple has publicly acknowledged its active participation in the creation of app content, stating that the commissions it charges on all App Store sales reflect the value of the "tools and software for the development, testing and distribution of developers' apps, and digital content" that it provides. Compl. ¶¶ 90, 92–97; *see also* Google Complaint ¶¶ 90, 91 ("The data that the Illegal Slot companies and the Platforms collect on monetization necessarily contribute to the structure and success of the Social Casino Enterprise.").

B. Booking Fees

The Platforms also "operate[ ] as the payment processor for all in-app purchases of virtual chips in the Illegal Slots. [The Platforms] collect[ ] the money players spend on virtual chips, take[ ] a cut for itself, and remit[ ] the rest to the Illegal Slots." Compl. ¶ 63; Facebook Complaint ¶ 60; Google Complaint ¶ 61. Plaintiffs argue that although the Platforms "do not determine the odds of winning any slot machine spins within the apps, they otherwise act much like the bookmakers in gambling parlance: accepting players' real money, provisioning casino chips to be wagered on illegal slot machine games, earning 30% of the gross sales for their contribution to the enterprise, and sometime later remitting the purchase amount (net of their fee) to the gambling game developers." Plaintiffs' Consolidated Opposition to CDA 230 Motions to Dismiss ("Opp.") at 5, Dkt. No. 104. When players run out of chips, they cannot continue playing the same slot machine game unless they purchase more chips. Compl. ¶¶ 61–63; Facebook Complaint ¶¶ 58–60; Google Complaint ¶¶ 59–61.

Virtual chips cannot be used outside of an individual Illegal Slots app. "The chips can only be used to (1) place wagers on slot machine spins, (2) place wagers on the few card game or bingo titles in the Illegal Slots app, or (3) give a "gift" of virtual chips to another account in the app. Substantially all virtual chips are used on slot machine spins." Compl. ¶ 65; Facebook Complaint ¶ 62; Google Complaint ¶ 63. As alleged by Plaintiffs, because the challenged apps derive most of their revenue from slot machine games, it is "substantially certain" that when a user buys virtual chips from the Platforms within a social casino app, those chips will be used to wager on a slot machine spin. Compl. ¶ 56; Facebook Complaint ¶ 53; Google Complaint ¶ 54.

C. Targeted Advertising

Plaintiffs allege that the Platforms are closely involved in social casinos' business strategies. For example, the Platforms and developers work together to "monitor the game activity and use the collected data to increase user spending." Compl. ¶ 91; Facebook Complaint ¶ 81; Google Complaint ¶ 88. Because the Platforms handle all payment processing for the social casinos, the developers often only have access to user data from the Platforms. Compl. ¶ 91; Facebook Complaint ¶ 81; Google Complaint ¶ 88. The Platforms and developers also "work together to target and exploit high-spending users, or 'whales.' " Compl. ¶ 92; Facebook Compliant ¶ 82; Google Complaint ¶ 89. For example, Apple "aids in the design and direction of targeted advertising, both on and within its App Store and other related Apple platforms, all aimed at driving new customers to [socials casinos] and retaining current gamblers." Compl. ¶ 94. Facebook provides "App Ads [which] allow Illegal slot companies to target high spending users and activate non-spending users." Facebook Complaint ¶ 84. Facebook also "sends targeted ads offering in-game rewards to users who invite their Facebook friends to play the [social casinos], and provides online "tournaments" which "driv[es] ... chip sales." Facebook Complaint ¶ 80. Google "aids in the design and direction of targeted advertising, both on Google.com, its larger Display Network, and within other apps and platforms, all aimed at driving new customers to the [social casinos] and retaining current gamblers." Google Complaint ¶ 91.

D. Claims Asserted

***3** Plaintiffs assert multiple claims against the Platforms. For instance, Plaintiffs pursue comparable claims under California, Alabama, Georgia, Connecticut, Illinois, Indiana, Minnesota, Mississippi, Missouri, New Mexico, New York, Ohio, and Oregon (among other states). These claims are similar—Plaintiffs pursue claims under unfair competition laws, unjust enrichment, illegal gambling and/or gambling loss laws. Importantly, the claims are asserted against the Platforms themselves. For example, Count I alleges that by hosting Illegal Slots within the meaning of California Penal Code § 330, Apple engaged in unfair competition within the meaning of California Business and Professions Code § 17200 by committing unlawful, unfair and fraudulent business acts and practices. *See* Compl. ¶¶ 148–71. Count II alleges, by hosting Illegal Slots, Apple was unjustly enriched to the detriment of Plaintiffs and profited immensely by providing marketing guidance, tools, and other assistances to the developers of social casinos and retaining a percentage of the money spent by consumers in social casinos. *See* Compl. ¶¶ 172–78. Count III alleges, by actively participating in the operation of social casinos by providing market guidance and helping create and develop the social casinos, Apple violated Alabama Code § 8-1-150(a). *See* Compl ¶¶ 179–86. Plaintiffs' claims of unfair competition, gambling violations, and unjust enrichment thus pursue the Platform's *individual* acts, not the acts of third-parties.

II. LEGAL STANDARD

"A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted tests the legal sufficiency of a claim." *Conservation Force v. Salazar*, 646 F.3d 1240, 1241–42 (9th Cir. 2011) (quotation marks and citation omitted). While a complaint need not contain detailed factual allegations, it "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible when it "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* When evaluating a Rule 12(b)(6) motion, the district court is limited to the allegations of the complaint, documents incorporated into the complaint by reference, and matters which are subject to judicial notice. *See La. Mun. Police Emps.' Ret. Sys. v. Wynn*, 829 F.3d 1048, 1063 (9th Cir. 2016) (citing *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007)).

III. DISCUSSION

The Platforms seek dismissal of the complaints filed against them without leave to amend, arguing that they are immune from suit under Section 230 of the Communications Decency Act of 1996 ("CDA"), 47 U.S.C. § 230. *See* Apple Inc.'s Notice of Motion and Rule 12(b)(6) Motion to Dismiss Based on Immunity Pursuant to Section 230 of the Communications Decency Act ("Apple MTD"), Dkt. No. 92; Defendants Google LLC and Google Payment Corp.'s Motion to Dismiss Master Complaint Under Section 230 of the Communications Decency Act ("Google MTD"), Dkt. No. 69; Motion of Defendant Meta Platforms,

Inc. to Dismiss Complaint Under Section 230 of the Communications Decency Act ("Facebook MTD"), Dkt. No. 99. Plaintiffs disagree, arguing that Section 230 of the CDA does not apply to the case at hand.

Section 230 of the CDA "protects certain internet-based actors from certain kinds of lawsuits." *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1099 (9th Cir. 2009). As relevant here, Section 230(c)(1) provides that "[n]o provider or user of an interactive computer service shall be treated as a 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 or local law that is inconsistent with this section." 47 U.S.C. § 230(e)(3). "The majority of federal circuits have interpreted the CDA to establish broad federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service." *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir. 2007) (quotation marks and citation omitted).

By its terms, section (c)(1) ensures that in *certain* cases, an internet service provider is not "treated" as the "publisher or speaker" of third-party content. Thus, Section 230's grant of immunity applies "only if the interactive computer service provider is not also an 'information content provider,' which is defined as someone who is 'responsible, in whole or in part, for the creation or development of" the offending content. *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1162 (9th Cir. 2008) (quoting 47 U.S.C. § 230(f)(3)). "The prototypical service qualifying for [CDA] immunity is an online messaging board (or bulletin board) on which Internet subscribers post comments and respond to comments posted by others." *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1097 (alteration in original) (quoting *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1266 (9th Cir. 2016)); *see also Doe v. Internet Brands, Inc.*, 824 F.3d 846, 850 (9th Cir. 2016) ("In general, [Section 230] protects websites from liability for material posted on the website by someone else.").

***4** In *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009), the Ninth Circuit created a three-prong test for Section 230 immunity. "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.' " *Dyroff*, 934 F.3d at 1097 (quoting *Barnes*, 570 F.3d at 1100–01). "When a plaintiff cannot allege enough facts to overcome Section 230 immunity, a plaintiff's claims should be dismissed." *Id.*

Importantly, and as will be demonstrated below, to assess these factors, the court must analyze how much control a website exercised over the offensive content. Practically speaking, the second and third factor tend to overlap in significant ways. The question of whether a plaintiff seeks to treat an interactive computer service as a publisher or speaker of third-party information (the second *Barnes* element) interacts in obvious ways with the question of whether the information provided is the information of a third-party (the third *Barnes* element). For instance, in *Fair Housing Valley Council of San Fernando Valley v. Roommates.com*, 521 F.3d 1157 (9th Cir. 2008) (en banc), liability turned on the website's prompts, which required users to create profiles that violated the Fair Housing Act. The website was not behaving as a "publisher or speaker" of third-party information, as it was publishing illegal content that it itself had elicited from others. It is for this reason that the Court also looks to the third element of *Barnes*, even while this action only concerns the second element of *Barnes*.

To determine whether Section 230 immunity applies, this Court must decide whether Plaintiffs' theory of liability would treat the Platforms as a publisher or speaker of third-party content. There is no dispute that prongs one and three are satisfied. Rather, Plaintiffs dispute the applicability of the second prong and argue that the second prong is not applicable because Plaintiffs seek to hold the Platforms liable for their own conduct.

A. The History of Section 230 CDA Immunity

Title V of the Telecommunications Act of 1996, Pub. L. No. 104-104, is known as the "Communications Decency Act of 1996" (the "CDA" or "the Act"). Its primary purpose was to "reduce regulation and encourage the rapid deployment of new telecommunications technologies." *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 857 (quotation marks omitted).

Section 230 was first offered as an amendment by Representatives Christopher Cox and Ron Wyden (*i.e.*, the "Cox-Wyden Amendment"). *See* 141 Cong. Rec. H8460-01 (Aug. 4, 1995). The primary goal of the amendment was to control the exposure of minors to indecent materials, specifically pornography, by immunizing interactive service providers that voluntarily censor offensive content posted on their sites. *Id.* It is for this reason that Section 230(c), the section of the amendment at issue, provides protection for "good Samaritan" blocking and screening of offensive material. *See* 47 U.S.C. § 230(c) (entitled "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material"). Pursuant to 47 U.S.C. § 230(c)(2):

> 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, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> ***5** (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).

By its plain language, Section 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, Section 230 precludes courts from entertaining claims that would place an interactive service provider in a publisher's role. A lawsuit that seeks to hold a provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content—are barred. This advances three purposes: protecting freedom of speech on the Internet, removing disincentives to voluntary private censorship, and encouraging the development of Internet commerce generally. *See Holomaxx Techs. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1103 (N.D. Cal. 2011) ("A principal purpose of the CDA is to encourage interactive service providers to engage in effective self-regulation of certain content. The Ninth Circuit has recognized that § 230 of the statute is 'designed ... to promote the free exchange of information and ideas over the internet and to encourage voluntary monitoring for offensive and obscene material.' " (quoting *Barnes*, 570 F.3d at 1099–1100)); *see also Green v. Am. Online (AOL)*, 318 F.3d 465, 472 (3d Cir. 2003) ("Section 230(c)(2) does not *require* AOL to restrict speech; rather it allows AOL to establish standards of decency without risking liability for doing so."); *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997); *Force v. Facebook Inc.*, 934 F.3d 53, 76 (Katzmann, C.J., concurring in part, dissenting in part) (analyzing the history of Section 230 and concluding that Section 230(c)(1) need not be interpreted to immunize websites' friend-and content-suggestion algorithms).

The legislative history of the Cox-Wyden Amendment makes clear that Congress enacted section 230 to remove the disincentives to self-regulation created by a New York state court decision, *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). There, the plaintiffs sued Prodigy, an interactive computer service provider, for defamatory comments made by an unidentified party on one of Prodigy's bulletin boards. The Court held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements, reasoning that Prodigy acted more like an original publisher than a distributor both because it advertised its practice of controlling content on its service and because it actively screened and edited messages posted on its bulletin boards.

The Cox-Wyden Amendment sought to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision. *See* 141 Cong. Rec. H8460-01 at 8469 (Aug. 4, 1995) ("Mr. Chairman, [the *Stratton Oakmont*] is backward. We want to encourage people like Prodigy ... to do everything possible for us, the customer, to help us control, at the portals of our computer, at the front door of our house, what comes in and what our children see."). Fearing that the specter of liability would deter service providers from blocking and screening offensive material, Congress enacted Section 230's broad immunity "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)(4). Section 230 also recognizes that interactive computer services offer a "forum for true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." *Id.* § 230(a)(1). It is the goal of Section 230 to preserve allow this "vibrant and competitive free market" to develop "unfettered by Federal or State regulation." *Id.* § 230(b)(2).

***6** Section 230 advanced an additional interest: to eliminate any chilling effect that tort liability would have on interactive service providers. Interactive computer services have millions of users. An immense amount of information is thus both posted and communicated on interactive sites. The imposition of tort liability would chill, if not eliminate, interactive service providers. It would be impossible for service providers to screen each of their millions of postings for possible problems. *Zeran*, 129 F.3d at 331. Such a responsibility would likely cause interactive service providers to severely restrict the number and type of messages posted, something that the CDA is expressly against. *See Reno*, 521 U.S. at 857 ("[The Act's] primary purpose was to reduce regulation and encourage the rapid deployment of new telecommunications technology." (quotation marks omitted)). In enacting Section 230, Congress chose to immunize service providers to avoid any restriction of interactive computer service providers' passive hosting of third-party speech. Accordingly, Section 230 sought to accomplish two objectives. Its broad grant of immunity both reduces obscenity on the Internet, by incentivizing service providers to review third-party content without fear of retribution, and precludes government censorship, by expressly barring service providers to be held liable for the speech of another. *See Batzel*, 333 F.3d at 1027–28.

B. Analysis of Section 230 CDA Immunity

The dispositive question in this case is whether the Platforms were "publishers or speakers" within the meaning of 47 U.S.C. § 230(c)(1). As established, through section 230, Congress granted most Internet services immunity from liability for publishing third-party material. To understand the boundaries of this immunity, the Court reviews several cases that have wrestled with the applicability of section 230 immunity. In doing so, the Court examines the motivations of section 230 and how these motivations interact with the holdings of this Circuit's case law. While this review is lengthy, it is important to understand how section 230 has evolved and whether it applies to the facts of this case. There is no doubt that the Internet of 1996, which boasted platforms that hosted "bulletin board" type websites, has changed. In examining this Circuit's case law, the Court attempts to understand the evolution of section 230 precedent and how that precedent has responded to the rapid and unforeseen changes to the Internet.

1. *Batzel v. Smith*

In *Batzel v. Smith*, the defendant, Ton Cremers, ran the Museum Security Network, which maintained a website and distributed an email newsletter via Listserv software. 333 F.3d 1018 (9th Cir. 2003) *superseded in part by statute on other grounds as stated in Breazeale v. Victim Servs., Inc.*, 878 F.3d 759, 766–67 (9th Cir. 2017). A handyman, Robert Smith, worked for Ellen Batzel at her home. *Id.* at 1020. Batzel told Smith that she was the granddaughter of one of Adolf Hitler's right-hand men. *Id.* at 1020–21. Batzel also told him that the paintings in her home were inherited. *Id.* at 1021. After "assembling these clues," Smith emailed the Museum Security Network, alleging that the painting in Batzel's home were looted during World War II based in part on Batzel's statements to him that she was a descendant of a Nazi and inherited the art. After making "some minor wording changes," Cremers posted the email on the network and sent it by a listserv to subscribers (including museum security investors, insurance investigators, and law-enforcement investigators, who use the network to track down stolen art). *Id.* at 1021–22. Batzel discovered the message and complained to the network operator, and ultimately sued Cremers, the network operator, the museum, and a security firm that advertised on the network "to redress her claimed reputational injuries." *Id.* at 1022.

Among other questions, the court examined whether Cremers was merely a "provider or user" of the Listserv, or rather an "information content provider," who "created" or "developed" the actionable content. *Id.* at 1031. The majority held that Cremers's minor alterations of Smith's email prior to its posting and his choice to publish the email, while rejecting others, did not make Cremers a co-information service provider. *Id.*; *see also* 47 U.S.C. § 230(f)(3) (defining "information content provider" to mean "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" (emphasis added)). The "development of information" means "something more substantial than merely editing portions of an e-mail and selecting material for publication." *Id.* Because Cremers did no more than select and make minor alterations to Smith's email, Cremers was not the content creator or provider

of Smith's email for Section 230 purposes. *Id.* The partial dissent diverged, arguing that immunity should not apply where a defendant has taken "an active role in selecting" information. *Id.* at 1040 (Gould, J., concurring in part and dissenting in part) ("I would hold that Cremers is *not* entitled to CDA immunity because Cremers actively selected Smith's e-mail message for publication.").

***7** While the majority and dissent reached different outcomes, they agreed that the relevant question in distinguishing "provider or user" from "information content provider" was the degree of editorial control exercised. Both focused on the degree of editorial control exercised and analyzed *what degree* of control is necessary to grant or deny immunity. For the majority, Cremers behaved like a publisher, acting with typical editorial discretion in deciding whether to publish or not. *See id.* at 1032 ("The scope of the immunity cannot turn on whether the publisher approaches the selection process as one of inclusion or removal, as the difference is one of method or degree, not substance."). In the majority's view, it would be nonsensical that Section 230 would not apply when its very purpose was to enable interactive computer providers to censor certain posts with impunity. *Id.* For the dissent, the discretion made Cremers a co-author as the discretion added Cremers' "imprimatur to [the email]." *Id.* at 1038 (Gould, J., dissenting). In the dissent's view, this advanced Congress's goal of encouraging providers to not publish offensive materials by requiring publishers, on the front end, to "filter" out obscene or offensive materials. *Id.* at 1040. Importantly, both the majority and the dissent's opinions contain a key principle—the question of whether immunity applies requires an analysis of what Section 230 sought to accomplish. Under the holding of *Batzel*, providing online intermediaries immunity for their inevitable (and editorial) responsibility of choosing which content to post, and for minor edits to that content, advances the twin aims of Section 230: it promotes a robust exchange of information and ideas over the Internet, while still encouraging platforms to voluntarily monitor their websites for third-party content that is offensive or obscene. *Id.* at 1026–30.

2. *Carafano v. Metrosplash.com, Inc.*

In *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1120 (9th Cir. 2003), the court considered "to what extent a computer match making service may be legally responsible for false content in a dating profile provided by someone posing as another person." There, an unidentified prankster placed a fraudulent personal ad on Matchmaker.com, a date matching website. *Id.* at 1121. To create a profile, members must complete a "detailed questionnaire containing both multiple-choice and essay questions." *Id.* The imposter created a profile for the plaintiff, Christianne Carafano. *Id.* Carafano, a popular actress, did not know of, consent to, or permit the posting of the profile. *Id.* The profile claimed that Carafano was looking for a "one-night stand" with a "hard and dominant" man with "a strong sexual appetite." *Id.* The profile used a contact email address, which when contacted, produced an automatic email reply that provided Carafano's home address and telephone number. *Id.* Carafano soon began receiving inappropriate voicemails, and when she returned home, she found a highly threatening and sexually explicit fax that also threatened her son. *Id.* Carafano ultimately learned of the profile, and sued Matchmaker.

The court held that Section 230 barred Carafano's claims for two reasons. First, the dating service was not the "information content provider" for the profiles on its website. *Id.* at 1124. "The fact that some of the content was formulated in response to Matchmaker's questionnaire does not alter this conclusion." *Id.* While the questionnaire facilitated the expression of information by individual users, the "selection of the content was left exclusively to the user." *Id.* The users, and not the website, were the "information content providers" because the users decided how to answer the questions provided. *Id.* That the website classified user characteristics into discrete categories and collected responses to specific essay questions did not transform the website into a "developer" of the "underlying information." *Id.* (citing *Gentry v. eBay, Inc.*, 99 Cal. App. 4th 816 (2002)). Thus, the website could not "be considered an 'information content provider' under the [CDA] because no profile ha[d] any content until a user actively create[d] it." *Id.* at 1124. Second, even if the dating services could be considered a content provider for publishing its customer's profiles, it was exempt from liability because it did not "create[ ] or develop[ ] the particular information at issue." *Id.* at 1125. The anonymous user entered the "critical information" (*i.e.*, Carafano's home address, movie credits, and the email address that revealed her phone number). *Id.* Likewise, the anonymous user created the profile with the sexually suggestive comments, "none of which bore more than a tenuous relationship to the actual questions asked." *Id.* Thus, the website did not play a "significant role in creating, developing, or 'transforming' the relevant information." *Id.*

***8** Much like *Batzel*, the court's inquiry focuses on the degree of control that the interactive computer service has over the content at issue. Importantly, the third-party provided information that was not solicited by the operator of the website. Indeed, Matchmaker's prompts sought information about the preparer of the profile—the individual answering the prompts—not about unwitting third parties. The questions neither suggested, encouraged, or solicited posting sensitive and personal information about another person, nor suggested, encouraged, or solicited the explicit information provided. In fact, the information as provided *despite* the website's rules and policies. Accordingly, immunity turned on the degree of control that Matchmaker exercised over the content generated on its website. Because Matchmaker was "neutral," in that it did not directly elicit the defamatory, private, or otherwise tortious or unlawful information at issue, it was immune under Section 230.

3. *Fair Housing Council of San Fernando Valley v. Roommates.com*

In *Fair Housing Valley Council of San Fernando Valley v. Roommates.com*, 521 F.3d 1157, 1161 (9th Cir. 2008) (en banc), the court "plumb[ed] the depths of immunity provided by section 230 of the [CDA]." There, the defendant, Roomates.com, operated an online roommate-matching service that was designed to match people renting out spare rooms with people looking for a place to live. *Id.* Before subscribers could search listings or post housing opportunities on Roommate's website, they had to create profiles, a process that required them to answer a series of questions. *Id.* "In addition to requesting basic information —such as name, location and email address—Roommate requires each subscriber to disclose his sex, sexual orientation and whether he would bring children to a household." *Id.* Each subscriber also had to describe "his preference[ ] in roommates with respect to the same three criteria: sex, sexual orientation, and [children]." *Id.* The site also encouraged subscribers to provide "Additional Comments" describing themselves and their desired roommate in an open-ended essay. *Id.* After a new subscriber completed the application, Roommate assembled his answers into a "profile page," which displayed the "subscriber's pseudonym, his description and his preferences." *Id.* at 1162. The Fair Housing Councils of the San Fernando Valley and San Diego ("the Councils") sued Roommate, alleging that Roommate's business violated the federal Fair Housing Act ("FHA") and California housing discrimination laws. *Id.* Roommate argued it was immune from suit under Section 230 of the CDA.

Using *Carafano* as a point of contrast, the *Roommates* court held that because Roommates.com had "materially contributed" to the unlawfulness of the content under the Fair Housing Act, it had "developed" the content within the meaning of CDA § 230(c)(1). *Id.* at 1167–68. "Here, the part of the profile that is alleged to offend the [FHA] and state housing discrimination laws—the information about sex, family status and sexual orientation—is provided by subscribers in response to Roommate's questions, which they cannot refuse to answer if they want to use defendant's services." *Id.* at 1166. By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate became more than a passive transmitter of information provided by others; it became the developer, at least in part, of that information. *Id.* "The CDA does not grant immunity for inducing third parties to express illegal preferences. Roommate's own acts—posting the questionnaire and requiring answers to it—are entirely its doing and thus section 230 of the CDA does not apply .... Roommate is entitled to no immunity." *Id.* at 1165.

The court further held that Roommate was not entitled to CDA immunity for the operation of its search system, which filtered listings, or its email notification system, which directed emails to subscribers according to discriminatory criteria. *Id.* at 1167. Roommate developed its search system, so it would steer users based on the preferences and personal characteristics that Roommate forced subscribers to disclose. *Id.* "If Roommate has no immunity for asking the discriminatory questions, ... it can certainly have no immunity for using the answers to the unlawful questions to limit who has access to housing." *Id.* Unlike search engines like Google, Yahoo!, or MSN, the Roommate search system used unlawful criteria to limit search results. As alleged in the complaint, Roommate's search was designed to make it harder, if not impossible, for individuals with certain protected characteristics to find housing—something the law prohibits. *Id.* In contrast, ordinary search engines are not developed to limit the scope of searches conducted on them and are not designed to achieve illegal ends. *Id.* Thus, such search engines "play no part in the 'development' of any unlawful searches." *Id.* (citing 47 U.S.C. § 230(f)(3)). Liability only attaches where a "website

helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct." *Id.* at 1168.

***9** The *Roommates* court analyzed its opinion in the context of *Batzel* and *Carafano.* Regarding *Batzel*, the court wrote

> The distinction drawn by Batzel anticipated the approach we take today. As Batzel explained, if the tipster tendered the material for posting online, then the editor's job was, essentially, to determine whether or not to prevent its posting—precisely the kind of activity for which section 230 was meant to provide immunity. *And any 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.* But if the editor publishes material that he does not believe was tendered to him for posting online, then he is the one making the affirmative decision to publish, and so he contributes materially to its allegedly unlawful dissemination. He is thus properly deemed a developer and not entitled to CDA immunity. *See Batzel*, 333 F.3d at 1033.

Roommates.com, 521 F.3d at 1171 (emphasis added) (citations omitted).

Regarding *Carafano*, the court attempted to clarify "the reasoning undergirding" the holding, which was "unduly broad." *Id.*

> In *Carafano*, ... [w]e correctly held that the website was immune, but incorrectly suggested that it could never be liable because "no [dating] profile has any content until a user actively creates it." .... [A] website operator may still contribute to the content's illegality and thus be liable as a developer. Providing immunity every time a website uses data initially obtained from third parties would eviscerate the exception to section 230 for "develop[ing]" unlawful content "in whole or in part."
>
> We believe a more plausible rationale for the unquestionably correct result in Carafano is this: The allegedly libelous content there—the false implication that Carafano was unchaste—was created and developed entirely by the malevolent user, without prompting or help from the website operator. To be sure, the website provided neutral tools, ... but the website did absolutely nothing to encourage the posting of defamatory content .... The claim against the website was, in effect, that it failed to review each user-created profile to ensure that it wasn't defamatory. *That is precisely the kind of activity for which Congress intended to grant absolution with the passage of section 230.* With respect to the defamatory content, the website operator was merely a passive conduit and thus could not be held liable for failing to detect and remove it.

Roommates.com, 521 F.3d at 1171–72 (emphasis added) (citations and footnote omitted).

Roommates.com makes clear that Section 230 immunity is premised on the activity of a website in eliciting the content at issue. If a website encourages or aids in the production of illegal content, the website cannot be said to be "neutral," and instead is properly said to be an "active" co-developer. By sharp contrast, if a website simply provides neutral tools, specifically designed to accomplish a benign objective, the website cannot be said to be a co-developer of illicit content. Again, at the heart of this logic is a simple understanding of what Section 230 sought to promote—free speech and fearless monitoring by websites. *See id.* at 1169 (contrasting the case with *Stratton Oakmont* and noting that "Rooomate is not being sued for removing some harmful messages while failing to remove others; instead, it is being sued for the predictable consequences of creating a website designed to solicit and enforcing housing preferences that are alleged to be illegal"). Indeed, the CDA, specifically Section 230, "was not meant to create a lawless no-man's-land on the Internet." *Id.* at 1164. [2]

4. *Barnes v. Yahoo!, Inc.*

***10** In *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1101 (9th Cir. 2009), the Court decided "how to determine when, for purposes of [Section 230], a plaintiff's theory of liability would treat a defendant as a publisher or speaker of third-party content." There, the plaintiff, Cecilia Barnes, sued Yahoo after it failed to take down fraudulent profiles that has been created by her ex-boyfriend. Barnes broke off a lengthy relationship with her boyfriend. He responded by posting profiles of her on a website run by Yahoo. The profiles contained nude photographs of Barnes and her boyfriend, taken without her knowledge, and open solicitation to engage in sexual intercourse. The ex-boyfriend, posing as Barnes, "chatted" with male correspondents in chat rooms. "Before long, men whom Barnes did not know were peppering her office with emails, phone calls, and personal visits, all in the expectation of sex." *Id.* at 1098. Barnes asked Yahoo to remove the profiles. Eventually, Yahoo promised it would take care of the profiles. Approximately two months passed without word from Yahoo, at which point Barnes filed this lawsuit against Yahoo in state court. Shortly thereafter, the profiles disappeared. Barnes pursued two theories of liability: (1) Yahoo negligently provided or failed to provide services that it undertook to provide and (2) Yahoo made a promise to her to remove the profiles but failed to do so. *Id.* at 1099. Yahoo moved to dismiss the action, contending that Section 230(c)(1) rendered it immune from liability.

The Ninth Circuit created a three-prong test for Section 230 immunity. *Id.* at 1100. "[I]t appears that subsection(c)(1) only 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." *Id.* at 1100–01 (footnote omitted). There was no dispute that Yahoo is a provider of an interactive computer service, and there was no dispute that the "information content" at issue was provided by another "information content provider." *Id.* at 1101. Thus, the "flashpoint" of the case was "the meaning of the 'publisher or speaker' part of subsection (c)(1)." *Id.*

The court first noted that Section 230 is not limited to defamation cases. *Id.*

> [W]hat matters is not the name of the cause of action—defamation versus negligence versus intentional infliction of emotional distress—what matters is whether the cause of action inherently requires the court to treat the defendant as the "publisher or speaker" of content provided by another. *To put it another way, courts must ask whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a "publisher or speaker."* If it does, section 230(c)(1) precludes liability.

Id. at 1101–02 (emphasis added); *see also id.* at 1102 (citing *Roommates.com*, 521 F.3d at 1170–71 and *Zeran*, 129 F.3d at 330 for support that "a publisher reviews material submitted for publication, perhaps edits it for style or technical fluency, and then decides whether to publish it").

The court determined that Yahoo was entitled to Section 230 immunity for Barnes's negligence claim, but not for her promissory estoppel claim. *Id.* at 1105, 1109. The negligence claim was based on Oregon law, which provided that one who undertakes to render services to another may be subject to liability from his failure to exercise reasonable care in that undertaking. *Id.* at 1102. Barnes argued that this theory "treat[ed] Yahoo not as a publisher, but rather as one who undertook to perform a service and did it negligently." *Id.* The court rejected this argument, concluding that Barnes could not "escape section 230(c) by labeling as a 'negligent undertaking' an action that is quintessentially that of a publisher." *Id.* at 1103. The court noted that the undertaking Yahoo allegedly failed to perform was the removal of the profiles from its website, an action that is quintessentially that of a publisher. "In other words, 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." *Id.* Because the choice, to publish or de-publish "can be boiled down to deciding whether to exclude material that third parties seek to post online," is paradigm publishing conduct, section 230(c)(1) barred the claim. *Id.* (quoting *Roommates.com*, 521 F.3d at 1170–71)).

***11** Regarding the promissory estoppel claim, the court determined that Section 230 did not apply. *Id.* at 1109. Observing that promissory estoppel "is a subset of a theory of recovery based on a breach of contract, the court concluded that "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.* at 1106–07. The court explained that "[c]ontract liability here would come not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication." *Id.* at 1107.

Critically, *Barnes* advances the underlying goals of Section 230. If Yahoo were found liable for negligent undertaking, there would be no way to distinguish it from a situation where someone attempts to hold a website liable for failing to remove inappropriate or defamatory content. This is exactly what Section 230 seeks to avoid. It immunizes interactive computer services for third-party offensive content. Here, Barnes's ex-boyfriend, the third party, posted inappropriate content on Yahoo, an interactive computer service. Barnes seeks to hold Yahoo liable for its negligent failure to remove the content. This is no different from *Stratton Oakmont.* It is for this reason that Yahoo's failure to remove the profiles was protected. It acted as an editor in deciding whether to withdraw the ex-boyfriend's content. *See id.* at 1102 ("[P]ublication involves reviewing, editing, and deciding whether to publish or withdraw from publication third-party content.").

5. *Doe v. Internet Brands, Inc.*

In *Doe v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. 2016), the court answered whether it would be inconsistent with Section 230(c)(1) for the State of California to require an interactive service provider to warn its users about the threat of a known sexual predator. There, the plaintiff, Jane Doe, was an aspiring model who posted information about herself on modelmayhem.com, a website owned by the defendant Internet Brands. Unbeknownst to Doe, two persons were using the website to identify targets for a rape scheme. The two people did not have their own profiles, they instead browsed profiles posted by models, contacted potential victims with fake identities posing as talent scouts, and lured the victims to south Florida for modeling auctions. *Id.* at 848. Once a victim arrived, the two people used a date rape drug to put her in a semi-catatonic state, raped her, and recorded the activity on videotape for sale and distribution as pornography. *Id.* Internet Brands purchased the website in 2008.

Shortly after the purchase, Internet Brands learned of how the two people were using the website. *See id.* at 849 ("As early as August, 2010, knew that two individuals, ... had been criminally charged in this scheme, and further knew from the criminal charges, the particular details of the scheme, including how MODELMAYHEM.COM had been used in the scheme and its members victimized."). In February 2011, several months after Internet Brands had learned about the criminal activity, the two people lured Doe to South Florida for a purported audition, where she was drugged, raped, and recorded. *Id.* Doe filed suit, asserting one count of negligent failure to warn. Internet Brands moved to dismiss, arguing that it was entitled to immunity under Section 230.

The court held that the CDA did not provide immunity against Plaintiff's negligent failure to warn claim. Unlike cases like *Carafano* and *Barnes*, Doe did not seek to hold Internet Brands liable as a "publisher or speaker" of content posted by a third-party on the Model Mayham website. The action did not turn on Internet Brands' monitoring or editing of its website. Instead, it turned on Internet Brands failure to warn Doe about information it obtained from an outside source. The duty to warn imposed by California law thus did not implicate Internet Brands' role as an editor or publisher of third-party content. *Id.* at 851.

***12** *Internet Brands* demonstrates that courts must carefully analyze a claimant's cause of action to determine if the action reaches the website's editorial functions. It also expresses limitations on section 230's scope. It is not enough that an interactive computer service be incidentally involved. Section 230(c)(1)'s purposes support this analysis. *Id.* The immunity provision was meant to protect websites against liability for failure to remove offensive content to promote free speech *and* to incentivize websites to self-monitor without fear that more liability will be imputed onto them. Doe's failure to warn claim "has nothing to do with Internet Brands' efforts, or lack thereof, to edit, monitor, or remove user generated content." *Id.* at 852. Critically, the court centered its decision around section 230's core purposes, while noting that "Congress has not provided an all-purpose get-out-of-jail-free card for businesses that publish user content on the internet, though any claims might have a marginal chilling effect." *Id.* at 853.

6. *HomeAway.com, Inc. v. City of Santa Monica*

In *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676 (9th Cir. 2019), Santa Monica attempted to manage the disruptions brought about by the rise of short-term rentals facilitated by innovative startups like HomeAway.com, Inc., and Airbnb.com by passing an ordinance regulating the short-term vacation rental market. The ordinance prohibited most types of short-term rentals, except for licensed home-shares. The ordinance imposed four obligations on hosting platforms directly. It required them to (1) collect and remit "Transient Occupancy Taxes," (2) disclose certain listing and booking information regularly, (3) refrain from completing any booking transaction for properties not licensed and listed on the City's registry, and (4) refrain from collecting or receiving a fee for "facilitating or providing services ancillary to a vacation rental or unregistered home-share." *Id.* at 680. HomeAway argued it was immune from suit under Section 230 of the CDA.

Only the second *Barnes* element was at issue in *HomeAway.* The court thus centered its analysis on whether the Ordinance treated HomeAway as a "publisher or speaker" in a manner that is barred by the CDA. *Id.* at 681. HomeAway argued that Section 230 preempted the ordinance because the ordinance implicitly required them to "monitor the content of a third-party listing and compare it against the City's short-term rental registry before allowing any booking to proceed." *Id.* at 682. Relying on *Internet Brands*, HomeAway argued that CDA immunity follows whenever a legal duty "affects" how an internet company "monitors" a website. *Id.*

The court rejected this argument, reasoning that HomeAway read *Internet Brands* too broadly.

> 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. We look instead to what the duty at issue actually requires: specifically, *whether the duty would necessarily require an internet company to monitor third-party content.*

Id. at 682 (citations omitted) (emphasis added).

Applying this standard, the court held that the ordinance fell outside of the CDA's immunity for three reasons. First, the ordinance did not require HomeAway (or any platform) to monitor third-party content. Instead, the ordinance prevented *the platforms* from undertaking a specific action—processing transactions for unregistered properties. *Id.* The ordinance did not require HomeAway to review content provided by the third-party hosts that list properties on the platform. Rather, "the only monitoring that appears necessary in order to comply with the Ordinance relates to incoming requests to complete a booking transaction—content that, while *resulting from* the third-party listings, is distinct, internal, and nonpublic." *Id.* Likewise, the duty to cross-reference bookings against Santa Monica's property registry did not require "monitoring" of third-party content because this conduct was not " 'publication' of third-party content." *Id.* (noting that HomeAway had no editorial control over the City's registry and that the ordinance could fairly charge parties with keeping abreast of the law).

***13** Second, the ordinance did not "proscribe, mandate, or even discuss the content of the listings that ... [p]latforms display on their websites." *Id.* The court rejected HomeAway's argument that in practice the ordinance would require them to remove third-party content because it would not make sense to keep "un-bookable listings" posted. *Id.* Even accepting that removing the listings would be the best option "from a business standpoint," nothing in the ordinance required this outcome. Because the underlying duty could have been satisfied without changes to content posted by the website's users—not postings by the website itself—Section 230 immunity did not apply. *Id.*

Finally, the ordinance did not impose "an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Id.* HomeAway argued that the ordinance conflicted with the CDA's goal to preserve a vibrant and competitive free Internet market unfettered by federal and state regulation. *Id.* The court rejected this argument, noting that the Ninth Circuit has "consistently eschewed an expansive reading of the statute that would render unlawful conduct 'magically ... lawful when [conducted] online,' and therefore 'giv[ing] online businesses an unfair advantage over their real-world counterparts." *Id.* (quoting *Roommate.com*, 521 F.3d at 1164 & n.15).

HomeAway, like *Roommates.com* and *Internet Brands*, confirms that Section 230 immunity is not limitless. It clarifies *Internet Brands*' holding that a platform's interaction with a third-party, without more, does not confer Section 230 immunity. Instead, immunity attaches when a court's intervention would *require* a platform to censor, edit, or post third-party content. That is, the relevant question is what outcome will a court's order achieve? Will the court reach a website's personal bad act, or will it seek to hold the website liable for failing to remedy the bad act of another? It is thus improper to view the attachment of immunity as an "exception" or a "rule." Section 230 immunity is circumstantial. Its applicability depends on whether the facts alleged attempt to hold a website liable for the bad acts of another. Therefore, courts must look closely at the facts alleged and ask who is responsible for the charged, illegal conduct. *Id.* at 683 ("[T]he CDA does not provide internet companies with a one-size-fits-all body of law."). Indeed, websites may not evade federal, state, and local regulation simply because they host third-party content. "Like their brick-and-mortar counterparts, internet companies must also comply with any number of local regulations concerning, for example, employment, tax, or zoning." *Id.*

Interestingly, *HomeAway* also anchors its interpretation of the CDA to *Stratton Oakmont*, the case that sparked section 230. In rejecting HomeAway's argument that denying immunity would defeat the purposes of the CDA, the court noted that "the [o]rdinance would not pose an obstacle to Congress's aim to encourage self-monitoring of third-party content." *Id.* at 683–84. While the CDA's immunity reaches beyond *Stratton Oakmont*, "the initial state court that sparked its enactment," the holding of *Stratton Oakmont* remains important to understanding the scope of the CDA. "Congress intended to 'spare interactive computer services [the] grim choice' between voluntarily filtering content and being subject to liability on the one hand, and 'ignoring all problematic posts altogether [to] escape liability.' " *Id.* (quoting *Roommates.com*, 521 F.3d at 1163–64). In holding that Section 230 did not immunize HomeAway, the court noted that Section 230's goals were not applicable because HomeAway "face[d] no liability for the *content* of the bookings; rather, any liability arises only from unlicensed bookings." *Id.* (emphasis added). Accordingly, when evaluating whether Section 230 applies, courts must assess if liability would force a platform to unwillingly censor third-party content as *Stratton Oakmont* required.

7. *Gonzalez v. Google LLC*

***14** In *Gonzalez v. Google LLC*, 2 F.4th 871 (9th Cir. 2021), the court addressed three appeals arising from separate acts of terrorism—one in Paris, one in Istanbul, and one in San Bernardino—in which Nohemi Gonzalez, Nawras Alassaf, Sierra Clayborn, Tin Nguyen, and Nicholas Thalasinos lost their lives. The foreign terrorist organization known as ISIS took credit for the attacks. The plaintiffs were members of the victims' families. The plaintiffs sued Google, Twitter, and Facebook for damages pursuant to the Anti-Terrorism Act, alleging that the social medica platforms were secondarily liable for the murders because the platforms knowingly allowed ISIS to post videos and other content to communicate its message of terror and to radicalize new recruits. *Id.* at 880. The plaintiffs specifically alleged that Google's YouTube platform used computer algorithms to match and suggest content to users based on their viewing history. This caused YouTube to recommend ISIS videos to users and enabled users to locate other ISIS content. *Id.* at 881–82. The plaintiffs also claimed that Google placed paid advertisements in proximity to ISIS-created content and shared the resulting ad revenue with ISIS. *Id.* at 880.

Regarding the second element [3] of the *Barnes* test, the court held that the plaintiffs' claims treated Google as the publisher or speaker of third-party material. The plaintiffs argued that their claims did not treat Google as the publisher, but instead imposed a "duty not to support terrorists." *Id.* at 891. As support, the plaintiffs argued that just as a brick-and-mortar retailer like Wal-

Mart is prevented from supplying materials to ISIS, Google is prohibited from supplying ISIS a communication platform. *Id.* In rejecting this argument, the court noted that the plaintiff's characterization of their claim as asserting a "duty not to support terrorists" overlooks that publication itself is the form of support Google allegedly provided to ISIS. *Id.* Problematically, the plaintiffs' claim—that Google failed to prevent ISIS from using its platform, and thereby allowed ISIS to disseminate its message of terror—seeks to impose liability based on ISIS's mere use of YouTube. Because "publishing encompasses 'any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online,'" the claim sought to treat Google as a publisher and was barred by Section 230. *Id.* (quoting *Roommates.com*, 521 F.3d at 1170–71).

Regarding the third element of the *Barnes* test, the court held that "an interactive computer service does not create or develop content by merely providing the public with access to its platform." *Id.* at 893. While the plaintiffs conceded that Google did not create any of the ISIS videos, they argued that Google created the "mosaics" by which the videos are delivered. *Id.* The plaintiffs argued that Google made a material contribution to the unlawfulness of ISIS content by pairing it with selected advertising and other videos because the "pairing" enhanced user engagement with the underlying content. *Id.* The court rejected this argument, reasoning that Ninth Circuit "case law forecloses the argument." *Id.*

Relying on *Dyroff v. Ultimate Software Group, Inc.*, 934 F.3d 1093 (9th Cir. 2019) and *Carafano*, the court concluded that Google's recommendation of content and its targeted advertising operated like a traditional search engine. *Gonzalez*, 2 F.4th at 894–95. Like a traditional search engine, which provides content in response to a user's queries, Google simply matched "what it knows about users based on their historical actions and sends third-party content to users that Google anticipates they will prefer." *Id.* at 895. The plaintiffs neither alleged that Google specifically targeted ISIS content nor designed its website to encourage videos that further the terrorist group's mission. *Id.* Instead, the plaintiffs allege that Google "provided a *neutral* platform that did not specify or prompt the type of content to be submitted, nor determine particular types of content its algorithms would promote." *Id.*; *see also Force v. Facebook, Inc.*, 934 F.3d 53, 70 (2d Cir. 2019) (holding that Facebook's algorithms may have made content more visible or available, but this did not amount to *developing* the underlying information).

***15** The plaintiffs also asserted a revenue-sharing theory of liability. *Gonzalez*, 2 F.4th at 897. This theory was premised on the allegation that because Google shared advertising revenue with ISIS, Google should be held directly liable for providing material support to ISIS and secondarily liable for providing substantial assistance to ISIS in violation of the Anti-Terrorism Act. *Id.* at 898. The court held that section 230 did not immunize Google from the claims premised on revenue-sharing.

The plaintiffs alleged that Google generated revenue by selling space through its AdSense program, including advertising space that appeared on YouTube. Through AdSense, Google sold advertising opportunities and displayed advertisements to YouTube viewers accessing other content. The plaintiffs alleged that each YouTube video was reviewed and approved prior to Google permitting advertisements to be placed on the video, and thus Google reviewed and approved the ISIS videos for advertising. The plaintiffs alleged that because Google approved ISIS videos for the AdSense programs, Google shared a percentage of the revenues generated from those advertisements with ISIS. *Id.*

The court concluded that these allegations were not directed to the publication of third-party information. *Id.* Instead, the allegations were premised on Google providing ISIS with material support by remitting money to ISIS. *Id.* Unlike the plaintiffs' other allegations, the revenue-sharing theory did not depend on the particular content ISIS placed on YouTube. The theory depended only on *Google's* unlawful payments of money to ISIS. *Id.*

Gonzalez reaffirms that section 230 does not apply to a platform's *own* bad acts. In distinguishing between the two sets of claims, the court premised immunity on control. "Perhaps the best indication that the [plaintiffs'] revenue-sharing allegations are not directed to any third-party content is that *Google's violation of the [Anti-Terrorism Act] could be remedied without changing any of the content posted by the YouTube's users.*" *Id.* (emphasis added). Underlying this reasoning is a foundational understanding of what Section 230 sought to protect: website operators from liability based on a third-party's bad acts.

> Section 230's use of the phrase "publisher or speaker" was prompted by a New York state-court decision that held an internet service provider legally responsible for a defamatory message posted to one of its message boards. *Roommates*, 521 F.3d at

1163 (*citing* *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished)). *Stratton Oakmont* concluded that the internet service provider "had become a 'publisher' under state law because it voluntarily *deleted* some messages from its message boards 'on the basis of offensiveness and bad taste,' and was therefore legally responsible for the content of defamatory messages that it failed to delete." *Id.* (emphasis added) (internal quotation marks omitted) (quoting *Stratton Oakmont*, 1995 WL 323710, at *4). The original goal of § 230 was modest. By passing § 230, Congress sought to allow interactive computer services "to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they didn't edit or delete." *Id.*

Gonzalez, 2 F.4th at 887. Accordingly, and as established by cases like *Roommates.com* and *Internet Brands*, liability turns on the degree of control that a website exercises over the offensive content. Section 230 is not limitless. While its origin demonstrates a preference for immunity, it is not meant to immunize a website's own bad acts. With this in mind, the Court applies the relevant Ninth Circuit law to the facts of this case.

C. Application of Section 230

***16** As noted, section 230 of the CDA "protects certain internet-based actors from certain kinds of lawsuits." *Barnes*, 570 F.3d at 1099. "The majority of federal circuits have interpreted the CDA to establish broad federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service." *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir. 2007) (quotation marks and citation omitted). Of course, and as analyzed, this grant of immunity is not unlimited. *See Roommates.com*, 521 F.3d at 1162 ("This grant of immunity applies only if the interactive computer service provider is not also an 'information content provider,' which is defined as someone who is 'responsible, in whole or in part, for the creation or development of' the offending content." (quoting 47 U.S.C. § 230(f)(3))).

As distilled from the above cases, a website does not become responsible for the development of a third-party's offensive content merely by providing "neutral tools" that a third-party might use to create the offensive content. *Id.* at 1169. Thus, to determine if Section 230 immunizes a website, the court must determine the degree to which the website contributed to "the alleged illegality of the conduct." *Id.* at 1168. In this sense, section 230 operates to prevent a website from being vicariously liable for the acts of a third-party contributor. The operative question is therefore: does the plaintiff seek to hold a website liable for its *own* bad conduct or for the bad conduct of another?

To answer this question, the Ninth Circuit created a three-prong test for Section 230 immunity. "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." *Barnes*, 570 F.3d at 1100–01. Only the second element of the *Barnes* test is at issue. The Parties agree that the Platforms are interactive computer services and that the applications at issue were created by third parties. However, as this Court noted above, there is significant overlap between the second and third elements of the *Barnes* test. Indeed, allegations that a platform helped develop or create illegal content through data-sharing are certainly relevant to understanding whether the platform behaved as a "publisher or speaker" of third-party content.

Plaintiffs assert three theories of liability. One is premised on a non-revenue theory of liability and argues that the Platforms are liable because they promoted the illegal casino applications in their App Stores and thus induced users to play the illegal games. This is of the same nature as the non-revenue-based claim discussed in *Gonzalez*. The remaining two are premised on revenue theories of liability and argue that the Platforms are liable for *their own* illegal acts of selling gambling chips and working with developers to increase user engagement to drive revenue.

- The Platforms are liable for their acts of "offering, categorizing, and promoting" social casino applications in their respective App Stores, and applying special rules to the social casino applications.

- To play the social casino apps, users must buy virtual chips through the Platforms. *See* Google Complaint ¶ 61; Apple Complaint ¶ 63; Facebook Complaint ¶ 60 (alleging that the Platforms operated as "the payment processor for all in-app purchases of virtual chips in the Illegal Slots"). These virtual chips can only be used inside the social casino apps, and "[s]ubstantially all virtual chips are used on slot machine spins." Google Complaint ¶ 63; Apple Complaint ¶ 65; Facebook Complaint ¶ 62. The Platforms thus aid in the exercise of illegal gambling by selling chips that are "substantially certain" to be "used to wager on a slot machine spin." Opp. at 6.

***17** • The Platforms are closely involved in social casinos' business strategies. For example, the Platforms and social casino app developers work together to "monitor the game activity and use the collected data to increase user spending." Google Complaint ¶ 88; Apple Complaint ¶ 91; Facebook Complaint ¶ 81. The Platforms and the developers also "work together to target and exploit high-spending users, or 'whales.' " Google Complaint ¶ 89; Apple Complaint ¶ 92; Facebook Complaint ¶ 82. For example, Apple aids in the design and direction of targeted advertising to retain users and attract new users, Apple Complaint ¶ 94; Facebook provides "App Ads" which allow Illegal Slot companies to target high spending users and activate non-spending users and sends targeted ads offering in-game rewards to users who invite their Facebook friends to play the social casino apps, Facebook ¶¶ 80, 84; and Google aids in the design and direction of targeted advertising aimed at attracting and retaining users of the social casino apps, Google Complaint ¶ 91.

Plaintiffs' first theory of liability, a non-revenue claim, is easily dismissed under section 230. The recommendations and notifications in *Dyroff* and *Gonzalez* are not meaningfully different than the promotions of the social casino apps provided by the Platforms in the cases at issue here. Allegations that the Platforms are liable for actions that rely on algorithms to "amplify and direct users to content," like the social casino apps, cannot withstand section 230's grant of immunity. *Gonzalez*, 2 F.4th 871; *Dyroff*, 934 F.3d at 1099 ("The recommendation and notification functions helped facilitate this user-to-user communication, but it did not materially contribute, as Plaintiff argues, to the alleged unlawfulness of the content.").

Unlike Plaintiffs' first theory of liability, which attempts to hold the Platforms liable in their "editorial" function, Plaintiffs' second theory of liability seeks to hold the Platforms liable for their own conduct. Importantly, the conduct identified by Plaintiffs in their complaints is alleged to be unlawful. As alleged, players must buy virtual chips from the Platforms app stores and may only use these chips in the casino apps. It is this sale of virtual chips that is alleged to be illegal. Plaintiffs neither take issue with the Platforms' universal 30% cut, nor the Platforms' virtual currency sale. Plaintiffs only assert that the Platforms role as a "bookie" is illegal. Plaintiffs therefore do not attempt to treat the Platforms as "the publisher or speaker" of third-party content, but rather seek to hold the Platforms responsible for their own illegal conduct—the sale of gambling chips. *Compare Taylor v. Apple, Inc.*, No. 46 Civ. Case 3:20-cv-03906-RS (N.D. Cal. Mar. 19, 2021) ("Plaintiffs' theory is that Apple is distributing games that are effectively slot machines—illegal under the California Penal Code.... Plaintiffs are seeking to hold Apple liable for selling allegedly illegal gaming devices, not for publishing or speaking information."), *with Coffee v. Google, LLC*, 2022 WL 94986, at *6 (N.D. Cal. Jan. 10, 2022) ("In the present case, Google's conduct in processing sales of virtual currency is not alleged to be illegal. To the contrary, the [Complaint] states that '[v]irtual currency is a type of *unregulated* digital currency that is only available in electronic form.' If indeed the sale of Loot Boxes is illegal, the facts alleged in the FAC indicate that such illegality *is committed by the developer who sells the Loot Box for virtual currency, not by Google.*" (second alteration in original) (emphasis added)).

Plaintiffs' second "revenue-based" theory of liability is like the revenue-based claim found actionable in *Gonzalez* and *HomeAway.* In *Gonzalez*, liability attached to Google's action of funding terrorism in violation of the Anti-Terrorism Act. In *HomeAway*, liability attached to the website's unlawful transactions for unregistered properties. Likewise, here, Plaintiffs seek to impose liability for the Platforms processing of *unlawful* transactions for *unlawful* gambling. Accordingly, the requested relief is grounded in the Platforms' own bad acts, not in the content of the social casino apps that the Platforms display on their websites.

***18** Plaintiffs' third theory of liability is admittedly the trickiest. To decide whether Plaintiffs attempt to hold the Platforms liable as "publishers or speakers" of third-party content, the Court must determine whether the Platforms operated in a manner that contributes to the alleged illegality. As distilled from the above analysis, the focus of this inquiry is on the

Platform's neutrality—are the tools provided neutral such that the third party is solely responsible for the alleged illegality *or* do the tools provided aid in and encourage the alleged illegality? Problematically, the third theory of liability is much like the "recommendations" found non-actionable in *Gonzalez*. Like the recommendations provided by YouTube, the Platforms' recommendations (*i.e.*, targeted advertisements) communicated to each user that the Platforms thought the user would be interested in the social casino apps. That the recommended connection was to an application openly engaged in illegal activity is of no consequence. On the other hand, the Platforms are alleged to not just have recommended content, but to have helped develop specific advertisements meant to attract users to the social casino apps. In this sense, Plaintiffs hold the Platforms liable for sharing data with the social casino app developers to make their illegal product more appealing and addicting. Further, Plaintiffs point out that the Platforms had an incentive to do so. The social casino apps bring the Platforms significant profits. Making the games more appealing and addicting through data driven analytics inures to the benefit of the Platforms. Nonetheless, unlike *Roommates.com*, where the website actively elicited responses that formed the basis of violations of the Fair Housing Act, Plaintiffs do not allege that the Platforms contribution of data and advertisements helped create and develop the application itself. Moreover, unlike *Internet Brands*, where conduct did not involve the website's behavior as a "website," this case directly turns on how the Platforms aid the social casino developers in developing social casino apps. The Platforms are thus acting in their role as a "platform." In this sense, the Platforms behavior is more like the editor in *Batzel.* Just as the editor in *Batzel* bettered the post by making minor edits and bettered the website by choosing which messages to post, the Platforms have behaved as "editors" by helping develop the social casino apps using big data to make the games more profitable and more addicting. Providing social casino developers with big data is like an editor providing edits or suggestions to a writer. Indeed, the Platforms sharing of data is comparable to the recommendations found non-actionable in *Gonzalez.* Because the Platforms sharing of data is fairly seen as a classic editorial role, section 230 immunizes this conduct.

The Court holds that Plaintiffs' first and third theories of liability must be dismissed under section 230. However, Plaintiffs' second theory of liability is not barred by section 230. The Court thus **GRANTS in part and DENIES in part** Defendants' respective motions to dismiss.

Finally, the Court joins other opinions that note that the history of section 230 does not support a reading of the CDA so expansive as to reach a websites-generated message and functions. *See, e.g., Gonzalez*, 2 F.4th at 913 (Berzon, J., concurring); *Force*, 934 F.3d at 76 (Katzmann, C.J., concurring in part and dissenting in part). As analyzed, the twin goals of section 230 do not support this broad reading. Immunizing a website's own targeted advertisements and algorithms does not advance a website's internal policing of indecent content or promoting third-party speech. The data-driven targeting of consumers by big social-media platforms can hardly be compared to the Internet of 1996. Platforms like Facebook, Google, and Apple are more than mere message boards, they are creators of content themselves, and they should be treated as such.

D. Interlocutory Appeal

Generally, an appellate court should not review a district court's ruling until after entry of final judgment. *See In re Cement Antitrust Litig.*, 673 F.2d 1020, 1026 (9th Cir. 1982). However, there is an important exception. 28 U.S.C. § 1292(b) allows a district judge to certify an order for interlocutory appeal.

Certification pursuant to 28 U.S.C § 1292(b) has been interpreted to depend on four factors. A district court may certify an order for interlocutory appeal if (1) "the appeal involves a controlling question of law," (2) there is a "substantial ground for difference of opinion" on that question, (3) "an immediate appeal would materially advance the ultimate termination of the litigation," and (4) failure to certify the order "would result in wasted litigation and expense." *See Hawaii ex rel. Louie v. JP Morgan Chase & Co.*, 921 F. Supp. 2d 1059 (D. Haw. 2013). A district court may certify an order *sua sponte. See* Fed. R. App. P. 5(a). After a district court certifies an order for interlocutory appeal, the circuit court must in its discretion decide whether to certify the appeal. *See* 28 U.S.C. § 1292(b). Interlocutory appeals are "applied sparingly and only in exceptional cases." *United States v. Woodbury*, 263 F.2d 784, 788 n. 11 (9th Cir. 1959). A district court generally should not permit such an appeal where

it "would prolong the litigation rather than advance its resolution." *Syufy Enter. v. Am. Multi–Cinema, Inc.*, 694 F. Supp. 725, 729 (N.D. Cal. 1988).

This case presents exceptional circumstances that are sufficient to justify an interlocutory appeal. Immediate appeal on the section 230 immunity issue would help advance this action and avoid unnecessary litigation. This case involves controlling questions of law, namely whether the Platforms are entitled to immunity for their hosting of the allegedly unlawful social casino apps. While the Court believes it has followed the Ninth Circuit's precedent on this complicated question, the Court finds that reasonable minds could differ as to the outcome of this case. Finally, the Court finds that immediate appeal would materially advance the ultimate termination of the litigation and would ensure that resources are not wasted on needless litigation and expenses. If the Ninth Circuit reverses this Court as to Plaintiffs' second theory of liability, the case is resolved in its entirety. However, if interlocutory appeal is not granted and the Ninth Circuit reverses this Court's holding as to Plaintiffs' second theory of liability after final judgment is entered, it would be a significant and needless waste of the Court and the Parties' resources.

IV. CONCLUSION

***19** For the foregoing reasons the Court **GRANTS in part and DENIES in part** Defendants' respective motions to dismiss. The Court *sua sponte* **CERTIFIES THIS ORDER FOR IMMEDIATE INTERLOCTUORY APPEAL.** This action is **STAYED** pending determination from the Ninth Circuit Court of Appeals as to whether it will accept certification. The Parties are **ORDERED** to file a joint status report with the Court after the Court of Appeals has decided whether to certify the interlocutory appeal or in six months, whichever occurs first.

IT IS SO ORDERED.

All Citations

Slip Copy, 2022 WL 4009918

Footnotes

1 For ease, the Court references the Master Complaint filed in the "Apple," 21-md-2985, docket as "Compl." and refers generally to that complaint, unless a specific citation to the other two complaints is needed.

2 Importantly, the majority held that immunity applied to the "Additional Comments" section of profile pages because Roommate did "not provide any specific guidance" or "urge subscribers to input discriminatory preferences" in this section. *Roommates.com*, 521 F.3d at 1173 ("This is precisely the kind of situation for which section 230 was designed to provide immunity.").

3 There was no dispute that the first element was met.