934 F.3d 1093
United States Court of Appeals, Ninth Circuit.

Kristanalea DYROFF, individually and on behalf of the estate of Wesley Greer, deceased,
Plaintiff-Appellant,
v.
The ULTIMATE SOFTWARE GROUP, INC.,
Defendant-Appellee.

No. 18-15175
|
Argued and Submitted June 4, 2019,
Seattle, Washington
|
Filed August 20, 2019

Attorneys and Law Firms

David F. Slade (argued), Carney Bates & Pulliam PLLC, Little Rock, Arkansas; Sin-Ting Mary Liu, Aylstock Witkin Kreis & Overholtz PLLC, Alameda, California; for Plaintiff-Appellant.

Jeffry A. Miller (argued), Lewis Brisbois Bisgaard & Smith LLP, San Diego, California;, Lewis Brisbois Bisgaard & Smith LLP, San Diego, California; Shawn A. Tolliver and Justin S. Kim, Lewis Brisbois Bisgaard & Smith LLP, San Francisco, California; for Defendant-Appellee.

Appeal from the United States District Court for the Northern District of California, Laurel D. Beeler, Magistrate Judge, Presiding, D.C. No. 3:17-cv-05359-LB

Before: Dorothy W. Nelson, Johnnie B. Rawlinson, and Carlos T. Bea, Circuit Judges.

OPINION

D.W. NELSON, Circuit Judge:

Plaintiff Kristanalea Dyroff appeals the district court's dismissal of her claims against Defendant The Ultimate Software Group ("Ultimate Software"), operator of the Experience Project website, for its alleged role in the death of her son, Wesley Greer. While the circumstances and facts of this case are no doubt tragic, we find that Ultimate Software is immune from liability under Section 230 of the Communications Decency Act. We therefore affirm.

BACKGROUND

This being an appeal from a motion to dismiss, we describe the case as Plaintiff presents it. We take her plausible allegations as true and draw all reasonable inferences in her favor.

Experience Project was a social networking website made up of various online communities or groups where users anonymously shared their first-person experiences, posted and answered questions, and interacted with other users about different topics. The site did not limit or promote the types of experiences users shared. The site's "blank box" approach to user content resulted in an array of topics and forums ranging from

"I like dogs" and "I am going to Stanford" to "I have lung cancer" and "I Love Heroin."

Users registered with the site anonymously; in other words, the site did not collect users' identifying information, including name, phone number, or mailing address. The site's operator, Ultimate Software, believed that anonymity would promote users to share more personal and authentic experiences without inhibition. Experience Project's founder stated, "We don't want to know [users'] real name, their phone number, what town they're from." *Id.* "The impetus behind this policy [of anonymity] was to encourage users to share experiences with the least amount of inhibition possible. The greater the anonymity, the more 'honest' the post. . . ."

Experience Project was live from 2007 until March 2016, during which its users shared 67 million experiences, made 15 million connections, and asked 5 million questions. Users could join groups and the site also recommended groups for users to join, based on the content of their posts and other attributes, using machine-learning algorithms. When a user posted content to a group, the site would send an email notification to the other users active in that group. The site generated revenue through advertisements and the sale of tokens that users used to post questions to other users in their groups.

Some of the site's functions, including user anonymity and grouping, facilitated illegal drug sales. Wesley Greer was involved in one such transaction,

which turned fatal. Wesley suffered from drug addiction, which began when a doctor overprescribed him opioid pain killers after a serious sports-related injury. After several unsuccessful rehabilitation attempts, Wesley bought what he believed to be heroin from a fellow Experience Project user. Wesley posted in a heroin-related group, "where can i [sic] score heroin in jacksonville, fl." The site sent him an email notification when another user, Hugo Margenat-Castro or "Potheadjuice," an Orlando-based drug dealer, posted in the same group. Wesley and Margenat-Castro connected off the site and Wesley bought heroin from Margenat-Castro on August 18, 2015.

Wesley died the next day from fentanyl toxicity. He did not know that the heroin Margenat-Castro sold him was laced with fentanyl. Margenat-Castro was ultimately arrested and prosecuted. He pleaded guilty in March 2017 admitting that he sold heroin laced with fentanyl while active on Experience Project.

In March 2016, Experience Project announced, in an open letter to its users, that it was shutting down. The letter expressed concern for the future of online privacy because of government overreach. It stated that the site always supported proper law enforcement efforts but recognized that it did not have the resources to respond to increased government information requests. The site shut down on April 21, 2016.

Plaintiff Kristanalea Dyroff, Wesley Greer's mother, filed a complaint in San Francisco Superior Court. She alleges that Ultimate Software: (1) allowed users to

traffic anonymously in illegal, deadly narcotics and to create groups dedicated to their sale and use; (2) steered users to additional groups dedicated to the sale and use of narcotics; (3) sent users alerts to posts within groups that were dedicated to the sale and use of narcotics; (4) permitted users to remain active accountholders despite evidence that they openly engaged in drug trafficking and that law enforcement had undertaken related investigations; and (5) demonstrated antipathy toward law enforcement efforts to stop illegal activity on Experience Project.

Ultimate Software removed the action from state court based on diversity jurisdiction and filed a motion to dismiss all claims under Federal Rule of Civil Procedure 12(b)(6). The district court granted the motion without prejudice. Dyroff filed a notice stating that she would not file an amended complaint and asked the district court to enter judgement. Dyroff timely appealed the judgment.

STANDARD OF REVIEW

We review de novo both a district court order dismissing a plaintiff's claims pursuant to Federal Rule of Civil Procedure 12(b)(6) and questions of statutory interpretation. *Fields v. Twitter, Inc.*, 881 F.3d 739, 743 (9th Cir. 2018). The Court must "accept all factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party." *Rowe v. Educ. Credit Mgmt. Corp*., 559 F.3d 1028, 1029-30 (9th Cir. 2009). Only a complaint that

states a plausible claim for relief may survive a motion to dismiss. *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009). Plausibility exists when a court may "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*.

DISCUSSION

Plaintiff argues that in granting the motion to dismiss, the district court made three errors. First, she argues, the district court erred when it held that Communications Decency Act (CDA) Section 230 immunizes Defendant Ultimate Software. Plaintiff reasons that Ultimate Software, as the operator of the Experience Project website, was an information content provider, as defined by the statute, because its recommendation and notification functions were "specifically designed to make subjective, editorial decisions about users based on their posts." Second, according to Plaintiff, the district court erred when it found that her allegations of collusion between Ultimate Software and drug dealers using Experience Project were not plausible. Her third argument is that the district court erred in finding that Ultimate Software owed no duty of care to her son, Wesley Greer, an Experience Project user. We affirm because the district court did not err in any of these respects.

I. CDA Section 230 Immunizes Ultimate Software from Plaintiff's Claims

The CDA provides that website operators are immune from liability for third-party information (or content, like the posts on Experience Project) unless the website operator "is responsible, in whole or in part, for the creation or development of [the] information." 47 U.S.C. §§ 230(c)(1) & (f)(3). Ultimate Software did not create content on Experience Project, in whole or in part. Accordingly, Ultimate Software, as the operator of Experience Project, is immune from liability under the CDA because its functions, including recommendations and notifications, were content-neutral tools used to facilitate communications. *See Fair Hous. Council of San Fernando Valley v. Roommates.com*, 521 F.3d 1157, 1167-69 (9th Cir 2008) (en banc).

A. Scope of CDA Section 230 Immunity

The CDA instructs us that "[n]o provider or user of an *interactive computer service* shall be treated as the publisher or speaker of any information provided by *another information content provider*." 47 U.S.C. § 230(c)(1) (emphasis added). The CDA defines an "interactive computer service" as

> [A]ny information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet

> and such systems operated or services offered by libraries or educational institutions.

47 U.S.C. § 230(f)(2).

On the other hand, an "information content provider" is

> [A]ny 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.

47 U.S.C. § 230(f)(3).

"The prototypical service qualifying for [CDA] immunity is an online messaging board (or bulletin board) on which Internet subscribers post comments and respond to comments posted by others." *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1266 (9th Cir. 2016) (internal quotations omitted). In other words, a website like Experience Project. Taking the relevant statutory definitions and case law in account, it becomes clear that, in general, Section 230(c)(1) "protects websites from liability [under state or local law] for material posted on the[ir] website[s] by someone else." *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 850 (9th Cir. 2016); *see also* 47 U.S.C. § 230(e)(3).

Combining the above principles, in *Barnes v. Yahoo!, Inc.*, we created three-prong test for Section 230 immunity. 570 F.3d 1096, 1100 (9th Cir. 2009). 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. When a plaintiff cannot allege enough facts to overcome Section 230 immunity, a plaintiff's claims should be dismissed. *See Kimzey*, 836 F.3d at 1268-71. Ultimate Software satisfies all three prongs of the test.

B. Section 230 Immunity—The *Barnes* test

1. Defendant is an Interactive Computer Service

We interpret the term "interactive computer service" expansively. *Kimzey*, 836 F.3d at 1268. Ultimate Software was an interactive computer service because it did not create or publish its own content under the plain language of the statute. Rather, Ultimate Software published Experience Project users' posts and did not materially contribute to its users' posts.

Millions of users, including Plaintiff's son, Wesley Greer, set up accounts on Experience Project, a website, to communicate with each other. Websites are the most common interactive computer services. *Kimzey*, 836 F.3d at 1268; *see also Roommates.com*, 521 F.3d at 1162 n.6 ("[t]oday, the most common interactive computer services are websites").

No binding legal authority supports Plaintiff's contention that Ultimate Software became an information content provider, losing its Section 230 immunity, by facilitating communication on Experience Project

through content-neutral website functions like group recommendations and post notifications. Ultimate Software, therefore, satisfies the first prong.

2. Plaintiff Treats Ultimate Software as a Publisher or Speaker of Other's Information/Content

An interactive computer service, like Ultimate Software, can also be an information content provider, but that is only relevant, for the purposes of Section 230 immunity, if the website it operates creates or develops the specific content at issue. *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1124 (9th Cir. 2003). Here, Ultimate Software was not an information content provider because it did not create or develop information (or content). 47 U.S.C. § 230(f)(3). Rather, it published information created or developed by third parties. Specifically, Experience Project did not create or develop the posts that led to Greer's death. Rather, it was Greer, himself, who posted "where can i [sic] score heroin in jacksonville, fl" on Experience Project. And it was the drug dealer, Margenat-Castro, who posted in response to Greer's post.

It is true that Ultimate Software used features and functions, including algorithms, to analyze user posts on Experience Project and recommended other user groups. This includes the heroin-related discussion group to which Greer posted and (through its emails and push notifications) to the drug dealer who sold him the fentanyl-laced heroin. Plaintiff, however,

cannot plead around Section 230 immunity by framing these website features as content. We have held that what matters is whether the claims "inherently require[] the court to treat the defendant as the 'publisher or speaker' of content provided by another." *Barnes*, 570 F.3d at 1102. If they do, then Section 230(c)(1) provides immunity from liability. *Id.*

By recommending user groups and sending email notifications, Ultimate Software, through its Experience Project website, was acting as a publisher of others' content. These functions—recommendations and notifications—are tools meant to facilitate the communication and content of others. They are not content in and of themselves.

Our recent decision, *HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676 (9th Cir. 2019) is of no help to Plaintiff. There, the City of Santa Monica required short-term vacation rentals to be licensed and imposed liability on vacation rental hosting platforms—HomeAway.com and Airbnb—that facilitated unlicensed short-term vacation rentals. *Id.* at 680. The platforms sued, alleging, among other things, that Section 230 immunized them from liability. *Id.* We found that HomeAway.com and Airbnb did not meet the second prong of the *Barnes* test because the Santa Monica ordinance did not "proscribe, mandate, or even discuss the content of the [website] listings" and required only that the website's transactions involve licensed properties. *Id.* at 683. In other words, the vacation rental platforms did not face liability for the content of their

listings; rather liability arose from facilitating unlicensed booking transactions.

Ultimate Software, therefore, satisfies the second prong of the *Barnes* test.

3. Ultimate Software Published Information/Content Provided by Another Information Content Provider

The third prong is also met because, as stated previously and as detailed in Plaintiff's complaint, the content at issue was created and developed by Greer and his drug dealer. Plaintiff's content "manipulation" theory is without support in the statute and case law. First, Plaintiff misreads *Roommates.com* when she argues it holds that a website develops content if it manipulates the content in a unique way through content-neutral tools.

The question in *Roommates.com* was whether Section 230 immunized a website, which matched people renting rooms with people looking for somewhere to live, from claims that it violated federal and state housing anti-discrimination laws by requiring subscribers to disclose, using dropdown menus and checkboxes, their sex, sexual orientation, and family status. *See Roommates.com*, 521 F.3d at 1161-2, 1165.

We answered "no" to this question. We rested our decision, however, on the fact that Roommates.com affirmatively required users to disclose information related to protected classes through discriminatory

questions and answer choices. As a result, this information, especially information related to a user's protected class, served as the focus of the registration process and, ultimately, became the cornerstone of each user's online profile. Moreover, the website designed its search function to guide users through the required discriminatory criteria. *Id*. at 1164, 1167. Under these set of facts, the website in *Roommates.com* was clearly the developer of the discriminatory content at issue. *Id.* at 1170.

In *Roommates.com*, we also identified the type of conduct that does not constitute the "development" of content under Section 230. *Id.* at 1169. For example, a housing website 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, does not become a developer of content if it does not *require* the use of that discriminatory criteria. *Id*. In other words, a website does not become a developer of content when it provides neutral tools that a user exploits to create a profile or perform a search using criteria that constitutes a protected class. *Id*. We, furthermore, concluded that "[w]here it is very clear that the website directly participates in developing the alleged illegality—as it is clear here with respect to [Roommates.com's] questions, answers and the resulting profile pages—immunity will be lost." However, "in cases of enhancement by . . . inference—such as with respect to the 'Additional Comments' [on Roommates.com]—[S]ection 230 must be interpreted to protect websites not merely from ultimate liability,

but from having to fight costly and protracted legal battles." *Id*. at 1174-75.

Here, Ultimate Software's functions on Experience Project most resemble the "Additional Comments" features in *Roommates.com* in that Experience Project users, including Wesley Greer, were not required to disclose that they were looking for heroin or other illegal drugs. Rather, users were given something along the lines of blank text boxes in which they could post and share experiences, questions, and answers. 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. *Roommates.com*, 521 F.3d at 1175; *see also Kimzey*, 836 F.3d at 1269 n.4 (the material contribution test makes a "'crucial distinction between, on the one hand, taking actions (traditional to publishers) that are necessary to the display of unwelcome and actionable content and, on the other hand, responsibility for what makes the displayed content illegal or actionable.'").

In summary, Plaintiff is unable to allege that Ultimate Software materially contributed to the content posted on Experience Project that led to Greer's death. Plaintiff cannot and does not plead that Ultimate Software required users to post specific content, made suggestions regarding the content of potential user posts, or contributed to making unlawful or objectionable user posts. Ultimate Software is entitled to immunity under the plain terms of Section 230 and our case law as a publisher of third-party content.

II. Plaintiff Does Not Plead Sufficient Facts to Show that Ultimate Software Colluded with Drug Dealers on Experience Project

The complaint's allegations as it relates to Plaintiff's "collusion" with bad actors does not establish an independent theory of liability. Rather, Plaintiff tries, again, to circumvent Section 230 immunity by alleging that Ultimate Software knew or should have known that users sold drugs on Experience Project, and it supported and protected these drug dealers through its anonymity policies. The district court characterized this claim well, stating "The idea is that Ultimate Software is less Match.com and more Silk Road (a notorious online platform for criminal activities, including selling illegal drugs)."

To advance this collusion and inducement theory, Plaintiff relies on a Washington Supreme Court decision, *J.S. v. Village Voice Media Holdings, L.L.C.*, 184 Wash. 2d 95, 359 P.3d 714 (2015) (en banc). In *Village Voice Media*, plaintiffs, minors featured in advertisements for sexual services, sued the operators of the website Backpage.com alleging, among other things, violations of state laws prohibiting the sexual exploitation of children. *Id.* at 98, 359 P.3d 714. The court held that plaintiffs sufficiently alleged that the website operators helped develop the illegal content and therefore were not immune from liability under Section 230. *Id.* at 103, 359 P.3d 714.

Specifically, the court pointed to allegations that Backpage.com required users to disclose certain information within its "escorts" section that encouraged the

sexual exploitation of children. *Id.* at 102, 359 P.3d 714. One such allegation is that Backpage.com's "content requirements [were] specifically designed to control the nature and context of [escort] advertisements so that pimps can continue to use Backpage.com to traffic in sex, including the trafficking of children." *Id.* at 102-03, 359 P.3d 714. In other words, the court found that the plaintiffs alleged enough facts such that it was plausible to infer that Backpage.com's content requirements—within the website's escort section—were designed to facilitate the prostitution of children.

Here, Ultimate Software's anonymity features along with its public statements expressing concern for internet privacy and detailing the burden of law enforcement information requests are not facts whose inferences, viewed in the light most favorable to Plaintiff, plausibly allege collusion with drug dealers or other bad actors. Today, online privacy is a ubiquitous public concern for both users and technology companies. These statements do not establish, on the part of Ultimate Software, antipathy to law enforcement, especially given the corresponding statements about always supporting "proper law enforcement requests."

Unlike the plaintiffs in *Village Voice Media*, Plaintiff here did not allege that Experience Project had a section for drug-related experiences on its website with specific content posting requirements that facilitated illegal drug transactions. Plaintiff's allegation that user anonymity equals promoting drug transactions is not plausible. *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. The district court was right to dismiss all claims

related to this supposed theory of liability because Ultimate Software is, as reasoned above, immune under Section 230.

III. Ultimate Software Did Not Owe a Duty to Plaintiff's Son

Ultimate Software owed Greer no duty of care because Experience Project's features amounted to content-neutral functions that did not create a risk of harm. Plaintiff rests her "failure to warn claim" on a misguided premise that misfeasance by Ultimate Software created a duty to Greer.

When analyzing a duty of care in the context of third-party acts, California courts distinguish between "misfeasance" and "nonfeasance." *Melton v. Boustred*, 183 Cal. App. 4th 521, 531, 107 Cal.Rptr.3d 481 (2010). Misfeasance is when a defendant makes the plaintiff's position worse while nonfeasance is when a defendant does not help a plaintiff. *Lugtu v. Cal. Highway Patrol*, 26 Cal. 4th 703, 716, 110 Cal.Rptr.2d 528, 28 P.3d 249 (2001). Misfeasance, unlike nonfeasance, creates an ordinary duty of care where none may have existed before. *See id*.

Ultimate Software did not make Plaintiff's son, Greer, worse off because the functions Plaintiff references—recommendations and notifications—were used regardless of the groups in which a user participated. No website could function if a duty of care was created when a website facilitates communication, in a content-neutral fashion, of its users' content. *See e.g.*, *Klayman*

v. Zuckerberg, 753 F.3d 1354, 1359-60 (D.C. Cir. 2014) (no special relationship between Facebook and its users). We decline to create such a relationship. Accordingly, the district was correct to dismiss Plaintiff's duty to warn claim.

CONCLUSION

For the preceding reasons, we **AFFIRM** the district court's order granting Defendant Ultimate Software's motion to dismiss.

2017 WL 5665670
United States District Court, N.D. California,
San Francisco Division.

Kristanalea DYROFF, Plaintiff,
v.
The ULTIMATE SOFTWARE GROUP, INC.,
Defendant.

Case No. 17-cv-05359-LB
|
Signed 11/26/2017

Attorneys and Law Firms

Sin-Ting Mary Liu, Aylstock Witkin Kreis & Overholtz PLLC, Alameda, CA, David F. Slade, Carney Bates & Pulliam, PLLC, Little Rock, AR, for Plaintiff.

David Eugene Russo, Shawn Adrian Toliver, Justin S. Kim, Lewis Brisbois Bisgaard & Smith LLP, San Francisco, CA, John Joseph Moura, Gilbert Kelly Crowley & Jennett LLP, Los Angeles, CA, for Defendant.

ORDER GRANTING MOTION TO DISMISS

Re: ECF No. 13

LAUREL BEELER, United States Magistrate Judge

INTRODUCTION

The plaintiff Kristanalea Dyroff, individually and on behalf of her son's estate, sued Ultimate Software after her son, 29-year-old Wesley Greer, died from an

overdose of heroin laced with fentanyl.[1] Mr. Greer allegedly bought the drug from a drug dealer that he met online through their respective posts on Ultimate Software's (now inactive) social-network website "Experience Project." Ms. Dyroff asserts seven state claims: (1) Negligence, (2) Wrongful Death, (3) Premises Liability, (4) Failure to Warn, (5) Civil Conspiracy, (6) Unjust Enrichment, and (7) a violation of the Drug Dealer Liability Act (Cal. Health & Safety Code §§ 11700*, et seq.*).[2] She predicates Ultimate Software's liability on its mining data from its users' posts and using its proprietary algorithms to understand the posts and to make recommendations, which in this case steered Mr. Greer toward heroin-related discussion groups and the drug dealer who ultimately sold him the fentanyl-laced heroin.[3] Ultimate Software removed the action from state court based on diversity jurisdiction[4] and moved to dismiss all claims under Federal Rule of Civil Procedure 12(b)(6).[5]

For all claims except claim four, Ultimate Software asserts immunity under the Communications Decency Act, 47 U.S.C. § 230(c)(1).[6] Section 230(c)(1) provides

---

[1] Compl.—ECF No. 1-1 at 5 (¶ 8), 19 (¶ 44). Record citations refer to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of documents.

[2] *Id.* at 26–37 (¶¶ 72–126).

[3] Opposition to Motion to Dismiss—ECF No. 15 at 12.

[4] Notice of Removal—ECF No. 1 at 1–3.

[5] Motion to Dismiss—ECF No. 13-1.

[6] *Id.* at 8.

immunity to website operators for third-party content on their website unless they are responsible, in whole or in part, for the creation or development of content. *Id.* §§ 230(c)(1) & (f)(3). The court dismisses the claim because Ultimate Software is immune under § 230(c)(1). Its "[content]-neutral tools" facilitated communication but did not create or develop it. *Fair Hous. Council of San Fernando Valley v. Roommates.com*, LLC, 521 F.3d 1157, 1167–69 (9th Cir. 2008) (en banc).

For claim four (negligent failure to warn), Ultimate Software asserts that a website has no duty to warn its users of criminal activity by other users and that Mr. Greer assumed the risk of the obviously dangerous activity of buying drugs from an anonymous Internet drug dealer.[7] A duty to warn can arise from a business's "special relationship" with its customers or from its own creation of risk. *McGarry v. Sax*, 158 Cal. App. 4th 983, 995 (2008). The court holds that Ultimate Software had no special relationship with Mr. Greer and did not create risk through its website functionalities or its interactions with law enforcement, and thus it had no duty to warn Mr. Greer about another user's criminal activity.

The court dismisses all claims without prejudice and with leave to amend.

* * *

[7] *Id.* at 18.

STATEMENT[8]

Experience Project[9] is a (now dormant) social-network site consisting of various "online communities" or "groups" where users anonymously share their first-person "experiences" with other users.[10] Experience Project's founder stated, "We don't want to know [a user's] real name, their phone number, what town they're from." "The impetus behind this policy [of anonymity] was to encourage users to share experiences with the least amount of inhibition possible. The greater the anonymity, the more 'honest' the post. . . ."[11]

Thus, Experience Project allowed users to register on the site with anonymous user names and thereafter join or start groups based on their experiences or interests, such as "I like dogs," "I have lung cancer," "I'm going to Stanford," or "I Love Heroin," and to post and discuss their personal experiences and interests to those groups.[12] After a user established an account and joined a group, the user could ask questions or answer

---

[8] The allegations in the "Statement" are from the plaintiff's complaint. *See* Compl.—ECF No. 1-1.

[9] The plaintiff initially named Experience Project and Kanjoya, Inc. as additional defendants. Comp.—ECF No. 1-1. In its notice of removal, Ultimate Software explained that it acquired the website Experience Project from Kanjoya, which now is a wholly owned subsidiary of Ultimate Software. Notice of Removal—ECF No. 1; Stipulation—ECF No. 18. The parties then stipulated to dismiss Experience Project and Kanjoya. Stipulation—ECF No. 18. Ultimate Software thus is the only defendant.

[10] Compl.—ECF No. 1-1 at 6 (¶ 12), 8 (¶ 18).

[11] *Id.* at 16 (¶ 36).

[12] *Id.* at 3 (¶ 2), 8 (¶ 18), 20 (¶ 54).

questions posed by other members.[13] Ultimate Software, using advanced data-mining algorithms, analyzed the posts and other user data to glean information, including the underlying intent and emotional state of the users.[14] Ultimate Software used this information both for its own commercial purposes (such as selling data sets to third parties) and to steer Experience Project users to other groups on its website through its proprietary recommendation functionality.[15] It also utilized email and other "push" notifications to alert users when a new post or response occurred.[16] As of May 2016, the website had over sixty-seven million "experiences shared."[17]

In 2007, when he was a college student, Mr. Greer suffered a knee injury. During his recovery, he was prescribed opioid painkillers and became addicted, first to opioids and then to heroin.[18] He began treatment in 2011, completing five separate rehab programs, but he relapsed each time.[19] By 2013, he had completed a faith-based program in Florida, remained clean, and continued living and working there.[20] In January 2015, the program was unable to hire him, and he left to run a halfway house. He was concerned that the

---

[13] *Id.* at 9 (¶ 21).

[14] *Id.* at 3 (¶ 2).

[15] *Id.* at 3 (¶ 2) and 9 (¶ 22).

[16] *Id.* at 5 (¶ 8), 20 (¶ 52), 25–26 (¶ 70).

[17] *Id.* at 9 (¶ 20).

[18] *Id.* at 19 (¶ 44.)

[19] *Id.* (¶ 45).

[20] *Id.* (¶ 46).

drug-seeking environment there endangered his sobriety, and in February 2015, he moved home to Brunswick, Georgia, to live with his mother and stepfather and help them renovate their house.[21]

In August 2015, Mr. Greer conducted a Google search to find heroin, and he was directed to the defendant's website "Experience Project."[22] He created an account with Experience Project, purchased "tokens" (which enabled him to post questions to other users), and posted to a group titled "where can i score heroin in jacksonville, fl."[23]

On August 17, 2015, Experience Project sent an email to Mr. Greer notifying him that "Someone posted a new update to the question 'where can i score heroin in jacksonville, fl,'" and providing a hyperlink and a URL directing him to the update.[24] This update (or a similar one) alerted Mr. Greer that another Experience Project user, Hugo Margenat-Castro, an Orlando-based drug dealer, had responded to Mr. Greer's post. Mr. Greer was able to obtain his phone number through Experience Project.[25] Mr. Greer called Mr. Margenat-Castro, and in the early hours of August 18, 2015, drove from Brunswick, Georgia, to Orlando, Florida, where he bought fentanyl-laced heroin from Mr.

---

[21] *Id.* (¶¶ 47–48).

[22] *Id.* at 20 (¶ 49).

[23] *Id.* at 20 (¶¶ 49–51).

[24] *Id.* at 20 (¶ 52).

[25] *Id.* at 20–21(¶¶ 53–55).

Margenat-Castro. He then returned to Brunswick.[26] On August 19, 2015, Mr. Greer died from fentanyl toxicity.[27]

In numerous earlier posts on Experience Project, Mr. Margenat-Castro offered heroin for sale in groups such as "I love Heroin" and "heroin in Orlando." He actually sold heroin mixed with fentanyl ("a fact that he hid in his posts" and "misrepresented as heroin"). Fentanyl is a synthetic opioid that is fifty times stronger than heroin.[28]

Before Mr. Greer's death, Mr. Margenat-Castro regularly used Experience Project to sell a mixture of heroin and fentanyl. Based on his activity on Experience Project, law-enforcement agencies conducted "controlled buys" of heroin from Mr. Margenat-Castro on March 31, 2015, and June 24, 2015, and Mr. Margenat-Castro was arrested on April 1, 2015, and June 25, 2015, for possession with intent to sell fentanyl, among other drugs, stemming from his sale of drugs on Experience Project's website.[29] Officers made another controlled buy from Mr. Margenat-Castro on September 3, 2015. They tied him to his Experience Project handle "Potheadjuice," confirmed through a toxicology report that the substance contained fentanyl, and obtained an arrest warrant on October 7, 2015.[30] In his March 2017

---

[26] *Id.* at 20–21 (¶¶ 54–55, 57).

[27] *Id.* at 21 (¶ 57).

[28] *Id.* at 5 (¶¶ 7–8), 20 (¶ 54), 22–23 (¶ 61).

[29] *Id.* at 22–23 (¶¶ 61, 63).

[30] *Id.* at 24 (¶ 67).

plea agreement, Mr. Margenat-Castro estimated that he sold ten bags of fentanyl-laced heroin every day (seven days a week) between January 2015 and October 2015 via Experience Project. He estimated selling roughly 1,400 bags of heroin laced with fentanyl.[31] Ms. Dyroff contends that by August 17, 2015, when her son bought the drugs from Mr. Margenat-Castro, Ultimate Software had actual or constructive knowledge of Mr. Margenat-Castro's trafficking fentanyl-laced heroin on Experience Project.[32]

Ms. Dyroff alleges that Ultimate Software operated Experience Project in an unlawful manner that facilitated extensive drug trafficking between drug dealers and drug buyers, even providing "reviews" of drug dealers who trafficked on Experience Project's website.[33] Specifically, she alleges that Ultimate Software:

> (1) allowed its Experience Project users to anonymously traffic in illegal deadly narcotics;
>
> (2) allowed users to create groups dedicated to the sale and use of such illegal narcotics;
>
> (3) steered users to "additional" groups dedicated to the sale of such narcotics (through the use of its advanced data-mining algorithms to manipulate and funnel vulnerable

---

[31] *Id.* at 21–22 (¶ 58), 23–24 (¶ 64).

[32] *Id.* at 22–24 (¶¶ 61, 63, 66).

[33] *Id.* at 13 (¶ 31), 25–26 (¶ 70), 26–27 (¶ 73), 27 (¶ 75).

individual users to harmful drug trafficking groups on Experience Project's website);

(4) sent users emails and other push notifications of new posts in those groups related to the sale of deadly narcotics;

(5) allowed Experience Project users to remain active account holders despite (a) the users' open drug trafficking on Experience Project's website, (b) Ultimate Software's knowledge of this (including knowledge acquired through its proprietary data-mining technology, which allowed it to analyze and understand its users' drug-trafficking posts) and (c) multiple law-enforcement actions against users related to their drug dealing on the Experience Project website;

(6) exhibited general and explicit antipathy towards law enforcement's efforts to curb illegal activity on Experience Project's website;[34] and

(7) received numerous information requests, subpoenas, and warrants from law enforcement and should have known about drug trafficking on its site by its users, including—by the time of her son's death—Mr. Margenat-Castro's sales of fentanyl-laced heroin.[35]

* * *

[34] *Id.* at 26–27 (¶ 73), 3–4 (¶¶ 2–3), 16–17 (¶ 38).

[35] *Id.* at 4 (¶ 5), 17 (¶ 39), 24 (¶ 65), 25 (¶ 70).

GOVERNING LAW

A complaint must contain a "short and plain statement of the claim showing that the pleader is entitled to relief" to give the defendant "fair notice" of what the claims are and the grounds upon which they rest. Fed. R. Civ. P. 8(a)(2); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). A complaint does not need detailed factual allegations, but "a plaintiff's obligation to provide the 'grounds' of his 'entitlement to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do. Factual allegations must be enough to raise a claim for relief above the speculative level. . . ." *Id.* (internal citations omitted).

To survive a motion to dismiss, a complaint must contain sufficient factual allegations, which when accepted as true, "'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (quoting *Twombly*, 550 U.S. at 557). "Where a complaint pleads facts that are 'merely consistent with' a defendant's liability, it 'stops short of the line between possibility and plausibility of "entitlement to relief."'" *Id.* (quoting *Twombly*, 550 U.S. at 557).

If a court dismisses a complaint, it generally should give leave to amend unless "the pleading could not possibly be cured by the allegation of other facts." *Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv. Inc.*, 911 F.2d 242, 247 (9th Cir. 1990). A court need not grant leave to amend if the court determines that permitting a plaintiff to amend would be futile. *See e.g.*, *Beckman v. Match.com, LLC*, 668 Fed. Appx. 759, 759 (9th Cir. 2016) (district court did not abuse its discretion when it determined that amendment of claims [barred by § 230 of the Communications Decency Act] would be futile) (citing *Saul v. United States*, 928 F.2d 829, 843 (9th Cir. 1991)); *Rutman Wine Co. v. E. & J. Gallo Winery*, 829 F.2d 729, 738 (9th Cir. 1987).

* * *

ANALYSIS

The next sections address (1) whether Ultimate Software has § 230(c)(1) immunity for all claims except claim four, the failure-to-warn claim, and (2) whether Ultimate Software had a duty to warn Mr. Greer that Mr. Margenat-Castro was selling fentanyl-laced heroin.

1. Section 230(c)(1) Immunity

For all claims except claim four, Ultimate Software asserts that as a website operator, it is immune from liability under the Communications Decency Act ("CDA"), 47 U.S.C. § 230(c)(1).[36] The CDA provides that

[36] Motion to Dismiss—ECF No. 13-1 at 8–15.

website operators are immune from liability for third-party "information" (such as the posts here) unless the website operator "is responsible, in whole or in part, for the creation or development of the information." *Id.* §§ 230(c)(1) & (f)(3). The plaintiff contends that Ultimate Software developed third-party information (or content) here by mining data from its users' posts and using its proprietary algorithms to understand the posts and to make recommendations, which in this case steered Mr. Greer toward heroin-related discussions and the drug dealer who sold him fentanyl-laced heroin.[37] The court holds that Ultimate Software is immune under § 230(c)(1). Only third parties posted content, and without more, Ultimate Software's providing content-neutral tools to facilitate communication does not create liability. *See Roommates.com*, 521 F.3d 1157 at 1167–69.

In the next sections, the court provides an overview of the CDA and applies the Act to Ms. Dyroff's claims.

1.1 Overview Of the Communications Decency Act

Under the CDA, (1) website operators generally have immunity from third-party content posted on their websites, but (2) they are not immune if they create or develop information, in whole or in part. 47 U.S.C. §§ 230(c)(1) & (f)(3).

---

[37] Opposition to Motion to Dismiss—ECF No. 15 at 12.

1.1.1 Immunity For Third-Party Content

First, website operators generally are immune from liability from third-party posts. *Id.* Under the CDA, "[n]o provider or user of an *interactive computer service* shall be treated as the publisher or speaker of any information provided by *another information content provider.*" 47 U.S.C. § 230(c)(1) (emphasis added). Moreover, "no [civil] liability may be imposed under any State or local law that is inconsistent" with § 230(c)(1). *Id.* § 230(e)(3).

The most common "interactive computer services" are websites. *Roommates.com*, 521 F.3d at 1162 n.6.[38] The CDA defines an "information content provider" as "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." 47 U.S.C. § 230(f)(3).

In general, then, § 230(c)(1) "protects websites from liability for material posted on the[ir] website[s] by someone else." *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 850 (9th Cir. 2016). More specifically, § 230(c)(1) "'immunizes providers of interactive computer services against liability arising from content created by third parties.'" *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1265 (2016) (quoting *Roommates.Com*, 521 F.3d at 1162).

---

[38] The definition "interactive computer service" is "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2).

Section 230(c) thus "overrides the traditional treatment of publishers, distributors, and speakers under statutory and common law." *Batzel v. Smith*, 333 F.3d 1018, 1026 (9th Cir. 2003). "The prototypical service qualifying for [CDA] immunity is an online messaging board (or bulletin board) on which Internet subscribers post comments and respond to comments posted by others.'" *Kimzey*, 836 F.3d at 1266 (quoting *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1195 (10th Cir. 2009)).

1.1.2 No Immunity for Websites That Create or Develop Content

But if a website operator "is responsible, in whole or in part, for the creation or development of information" on its website, then it is an "information content provider," and it does not have immunity from liability for that information. 47 U.S.C. §§ 230(c)(1) & (f)(3); *Roommates.com*, 521 F.3d at 1165. As the Ninth Circuit has explained, the CDA "does not declare 'a general immunity from liability deriving from third-party content.'" *Internet Brands*, 824 F.3d at 852 (quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100 (9th Cir. 2009)). Nor was it "meant to create a lawless no-man's land on the Internet." *Roommates.com*, 521 F.3d at 1164.

In *Roommates.com*, the Ninth Circuit considered whether Roommates.com created content, found that it did (at least "in part"), and concluded that it was not entitled to § 230(c)(1) immunity for the content that it created. 521 F.3d at 1165. Roommates.com operated a

website that matched people renting rooms to people looking for a place to live. *Id.* at 1161. It required subscribers to create profiles and answer questions—about themselves and preferences in roommates—regarding criteria including sex, sexual orientation, and whether they would bring children to the household. *Id.* at 1161. The Fair Housing Councils of the San Fernando Valley and San Diego sued Roommates.com, alleging that it violated the federal Fair Housing Act and California housing-discrimination laws. *Id.* at 1162. Roommates.com asserted that it had immunity under § 230(c)(1).

In its *en banc* decision, the Ninth Circuit held that Roommates.com was not immune for eliciting discriminatory preferences that violated federal and state fair-housing laws:

> 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[39] [became] much more than a passive transmitter of information provided by others; it [became] the developer, at least in part, of that information. And section 230 provides immunity only if the interactive computer service does not 'creat[e] or develop[ ]' the information 'in whole or in part.'"

Id. at 1166 (citing 47 U.S.C. § 230(f)(3)). Accordingly, the court held, "the fact that [third-party website]

---

[39] The opinion refers to "Roommate" (as opposed to the plural Roommates, which is the spelling in the case caption and in the company's name Roommates.com).

users are information content providers does not preclude [the website itself] from *also* being an information content provider by helping 'develop' at least 'in part' the information" at issue. *Roommates.com*, 521 F.3d at 1165 (emphasis in the original). This means that

> [a] website operator can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is 'responsible, in whole or in part' for creating or developing, the website is also a content provider."

Id. at 1162 (quoting 47 U.S.C. § 230(f)(3)). "Thus, a website may be immune from liability for some of the content it displays to the public but be subject to liability for other content." *Id.* at 1162–63. As the court summed up, "[t]he 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 to them. Roommate is entitled to no immunity." *Id.* at 1165.

By contrast, the court immunized Roommates.com from liability for statements that subscribers independently displayed in an "Additional Comments" section of their profile. *Id.* at 1173–74. Roommates.com prompted subscribers to "personalize your profile by writing a paragraph or two describing yourself and what you are looking for in a roommate." *Id.* at 1173.

"[S]ubscribers provide[d] a variety of provocative and often very revealing answers," such as their preferences for roommates' sex, sexual orientation, and religion. *Id.* Roommates.com published the statements as written, did not provide guidance about content, and did not "urge subscribers to input discriminatory preferences." *Id.* at 1173–74. The court held that Roommates.com was "not responsible, in whole or in part, for the development of this content, which comes entirely from subscribers and is passively displayed by Roommate." *Id.* at 1174. "Without reviewing every post, Roommate would have no way to distinguish unlawful discriminatory preferences from perfectly legitimate statements." *Id.* Moreover, there could be no "doubt that this information was tendered to Roommate for publication online." *Id.* "This," the Ninth Circuit held, "is precisely the kind of situation for which section 230 was designed to provide immunity." *Id.*

As an illustration of the difference between publishing third-party content (entitling the website operator to immunity) and developing content (resulting in no immunity), the Ninth Circuit distinguished Roommates.com's search function from generic search engines. *Id.* at 1167. Roommates.com steered users based on discriminatory criteria, thereby limiting search results and forcing users to participate in its discriminatory process. *Id.* By contrast, generic search engines such as Google, Yahoo!, and MSN "do not use unlawful criteria to limit the scope of the searches[,] . . . [are not] designed to achieve illegal ends [unlike Roommates.com's alleged search function, and thus] . . . play no part in

the 'development' of any unlawful searches." *Id.* at 1167. The court concluded that "providing neutral tools to carry out what may be unlawful or illicit [activities] does not amount to 'development' for purposes of the immunity exception." *Id.* at 1168–69.

1.1.3 Three-Element Test for Immunity Under § 230(c)(1)

Separated into its elements, § 230(c)(1) 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 [here, Mr. Margenat-Castro].'" *Kimzey*, 836 F.3d at 1268 (quoting *Barnes*, 570 F.3d at 1100–01).

1.2 Application Of the Three-Element Test To Ms. Dyroff's Claims

1.2.1 Is Ultimate Software a Provider of an Interactive Computer Service?

The first element is whether Experience Project is an "interactive computer service." It is undisputed that it is.[40] *See Roommates.com*, 521 F.3d at 1162 (websites are the most common "interactive computer services").

---

[40] *See, e.g.*, Compl.—ECF No. 1-1 at 8 (¶ 18).

1.2.2 Does the Plaintiff Seek To Treat Ultimate Software as a Publisher?

The second element is whether Ms. Dyroff seeks to treat Ultimate Software as a speaker or publisher. Her claims predicate Ultimate Software's liability on its tools and functionalities. More specifically, she alleges that Ultimate Software creates or develops information by mining data from its users' posts, using its proprietary algorithms to analyze posts and recommend other user groups, and—in this case—steering Mr. Greer to heroin-related discussion groups and (through its emails and push notifications) to the drug dealer who sold him the fentanyl-laced heroin.[41]

The issue here is whether plaintiffs can plead around § 230(c)(1) immunity by basing their claims on the website's tools, rather than the website operator's role as a publisher of the third-party content. The Ninth Circuit has held that what matters is whether the claims "inherently require[] the court to treat the defendant as the 'publisher or speaker' of content provided by another." *Barnes*, 570 F.3d at 1102. If they do, then § 230(c)(1) precludes liability. *Id.*; *accord Airbnb, Inc. v. City & County of San Francisco*, 217 F.Supp.3d 1066, 1074 (2016) (citing *Barnes*, 570 F.3d at 1102).

In similar cases, courts have rejected plaintiffs' attempts to plead around immunity by basing liability on a website's tools. *See, e.g.*, *Gonzalez v. Google, Inc.*, No. 16-cv-03282-DMR, 2017 WL 4773366, at *10–11 (N.D. Cal. October 23, 2017) (rejecting the plaintiffs'

[41] Opposition to Motion to Dismiss—ECF No. 15 at 12.

argument that claims were not based [sic] Google's publishing third-party content from ISIS but instead were based on Google's "provid[ing] ISIS followers with access to powerful tools and equipment to publish their own content"); *Fields v. Twitter*, 217 F. Supp. 3d 1116, 1121–22 (N.D. Cal. 2016)*, appeal docketed*, No. 16-17165 (9th Cir. Nov. 25, 2016) (rejecting the plaintiffs' argument that their claims were not based on Twitter's publishing third-party content by ISIS but instead were based on Twitter's allowing ISIS members to sign up for Twitter accounts).

The court holds that Ms. Dyroff's claims at their core seek liability for publishing third-party content. Element two of the § 230(c)(1) test is satisfied.

1.2.3 Is the Harmful Content "Third-Party Content"?

The third element is whether the content is third-party content. A third party—Mr. Margenat-Castro—posted on Experience Project. The issue is whether his posts and other allegedly harmful content are third-party content, which means that § 230(c)(1) bars the claims against Ultimate Software, or whether Ultimate Software "is responsible, in whole or in part, for the creation or development of the information," which means that § 230(c)(1) does not bar the claims. 47 U.S.C. § 230(c)(1) & (f)(3).

Ms. Dyroff contends that the court should deem Ultimate Software to have "developed" the harmful content, at least in part, for two reasons: (1) its tools,

design, and functionality abetted the content, at least in part, by recommending heroin-related discussions and steering Mr. Greer to Mr. Margenat-Castro's posts; and (2) Ultimate Software is not merely a passive conduit for its users' posts because it knew that Experience Project was an online market for drug dealers and users, and it shielded the bad actors through its anonymity policies and antipathy to law enforcement.[42]

1.2.3.1 Ultimate Software's Use of Tools to Develop Content

Ms. Dyroff contends that a website does not need to co-author a user's posts to "develop" the content and thus be responsible for the posts.[43] *See* 47 U.S.C. § 230(f)(3). She asserts that a website "develops" content otherwise created by third-party users (and loses immunity) when it "materially manipulates that content, including by passively directing its creation or by improperly using the content, after the fact."[44] "This manipulation can take myriad forms, including guiding the content's generation, either through posting guidelines that signal or direct the poster, content requirements for posts, or even *post-hoc* use of content that was generated in whole or in party by a third party."[45]

---

[42] *Id.* at 13–23.

[43] *Id.* at 17.

[44] *Id.* at 13 (citing *Roommates.com*, 521 F.3d at 1168).

[45] *Id.* (citations omitted).

Her specific allegations about Ultimate Software's development of information are as follows. Ultimate Software used "data mining" techniques and "machine learning" algorithms and tools to collect, analyze, and "learn[] the meaning and intent behind posts" in order to "recommend" and "steer" vulnerable users, like her son, to forums frequented by drug users and dealers.[46] By identifying interested users and using its "recommendation functionality" to steer them to drug-related "groups" or "online communities," Ultimate Software kept the users "engaged on the site" for Ultimate Software's financial gain (through online ad revenues, gathering more valuable user data, and other means).[47] This system—combined with Experience Project's anonymous registration and its email-notification functionality that alerted users when groups received a new post or reply—"created an environment where vulnerable addicts were subjected to a feedback loop of continual entreaties to connect with drug dealers."[48]

The ordinary rule is that Ultimate Software is immune from liability for third-party content on its website unless it is "responsible, in whole or in part, for the creation or development of information." 47 U.S.C.

---

[46] *Id.* at 7, 9–10 (citing Compl.—ECF No. 1-1 at 9–12 (¶¶ 22–23, 27–28)), 18–19 (citing Compl.—ECF No. 1-1 at 5 (¶¶ 7–8), 11–19 (¶¶ 26–42), 20 (¶¶ 52–53), 25–26 (¶¶ 70–71)).

[47] *Id.* at 7, 17–19; Compl.—ECF No. 1-1 at 3 (¶ 2), 4–5 (¶¶ 6–8), 9–12 (¶¶ 22–23, 25, 27–29), 18–19 (¶ 42), 22 (¶ 59), 25–26 (¶¶ 70–71), 27 (¶ 75), 30 (¶ 90), 32 (¶ 96), 34 (¶ 107), 35 (¶ 114), 36 (¶ 116).

[48] *Id.* at 10 (citing Compl.—ECF No. 1-1 at 11–16 (¶¶ 26–35)).

§§ 230(c)(1) & (f)(3). Here, only third parties posted information on Experience Project, and the website operator did not solicit unlawful information or otherwise create or develop content. Ultimate Software is not an "information content provider" merely because its content-neutral tools (such as its algorithms and push notifications) steer users to unlawful content. *Roommates.com*, 521 F.3d at 1167. The following points support this conclusion.

First, making recommendations to website users and alerting them to posts are ordinary, neutral functions of social-network websites. To support her contrary contention that Ultimate Software's functionalities create or develop information, Ms. Dyroff relies on *Roommates.com* and *Anthony v. Yahoo! Inc.*, but she does not allege any facts comparable to the facts in those cases.[49]

In *Roommates.com*, the website operator created a questionnaire, provided a limited set of pre-populated (and unlawful) answers as a condition of accessing the website and its services, and steered users based on the pre-populated answers. 521 F.3d at 1166–67. By these acts, Roommates.com "[became] much more than a passive transmitter of information provided by others; it [became] the developer, at least in part, of that information. And section 230 provides immunity only if the interactive computer service does not 'creat[e] or

---

[49] *Id.* at 13–16 (citing *Roommates.com*, 521 F.3d at 1161–62, 1165, 1167–68, and *Anthony v. Yahoo!*, 421 F. Supp. 2d 1257, 1262–63 (N.D. Cal. 2006)).

develop[]' the information 'in whole or in part.'" *Id.* at 1166 (quoting 47 U.S.C. § 230(f)(3)). By contrast, here, Ultimate Software did not solicit unlawful content from its third-party users and merely provided content-neutral social-network functionalities—recommendations and notifications about posts. "Providing neutral tools for navigating websites is fully protected by CDA immunity, absent substantial affirmative conduct on the part of the website creator promoting the use of such tools for unlawful purposes." *Id.* at 1174 n.37; *accord Gonzalez*, 2017 WL 4773366, at *11 (rejecting claim that Google was liable because YouTube's website "functionality" purportedly facilitated ISIS's communication of its message, which resulted in great harm); *Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140, 158 (E.D.N.Y. May 18, 2017) (rejecting claim that Facebook provided a tool to support terrorist organizations); *Fields*, 217 F. Supp. 3d 1120–23 (rejecting claim that Twitter provided ISIS with material support by permitting it to sign up for accounts). Ms. Dyroff does not plausibly allege that Ultimate Software "promoted the use of [its neutral] tools for unlawful purposes." *Roommates.com*, 521 F.3d at 1174 n.37.

Similarly, Ms. Dyroff relies on *Anthony v. Yahoo!*, but does not allege facts comparable to those in that case. Yahoo! allegedly created fake user profiles and sent them—along with actual user profiles of former subscribers—to current website users to try to persuade them to renew their lapsed subscriptions to Yahoo's online dating service. 421 F. Supp. 2d at 1262. Assuming the allegations to be true for its Rule

12(b)(6) inquiry, the court held that Yahoo! was not immune under § 230(c)(1) for two reasons. *Id.* First, Yahoo! created content in the form of the false profiles and thus was an "information content provider." *Id.* at 1262–63. Second, with actual knowledge of the false profiles—including those of former users—Yahoo! used the content to (allegedly) commit fraud and thus was responsible for its misrepresentations. *Id.* (collecting cases on § 230(c)(1) immunity). By contrast, here, Ultimate Software did not create or use unlawful content and merely provided its neutral social-network functionalities.

Second, it is the users' voluntary inputs that create the content on Experience Project, not Ultimate Software's proprietary algorithms. *See, e.g.*, *Kimzey*, 836 F.3d at 1268–70 (Yelp!'s "star-rating system is best characterized as the kind of 'neutral tool[]' operating on 'voluntary inputs' that we determined that does not amount to content development or creation in *Roommates.com*, 521 F.3d at 1172."). Moreover, even if a tool "'facilitates the expression of [harmful or unlawful] information,'" it is considered neutral "so long as users ultimately determine what content to post, such that the tool merely provides 'a framework that could be utilized for proper or improper purposes.'" *Goddard v. Google, Inc.*, 640 F. Supp. 2d 1193, 1195 (N.D. Cal. 2009) (rejecting claim that Google's "Keyword Tool"—which provides options that advertisers can adopt or reject at their discretion—created liability for subsequent postings by the advertisers of false or misleading advertisements) (citing *Roommates.com*, 521 F.3d at

1172); *Carafano*, 339 F.3d at 1121, 1124; *see also Klayman v. Zuckerberg*, 753 F.3d 1354, 1358 (D.C. Cir. 2014) ("a website does not create or develop content when it merely provides a neutral means by which third parties can post information of their own independent choosing online").

Third, the result holds even when a website collects information about users and classifies user characteristics. The website is immune, and not an "information content provider," as long as users generate all content. *Carafano*, 339 F.3d at 1121, 1124 (online dating site used questionnaires to collect information about members; "the fact that [the site] classifies user characteristics into discrete categories and collects responses to specific essay questions does not transform the [site] into a 'developer' of the 'underlying misinformation.' ").

The court follows these cases and holds that the Experience Project website's alleged functionalities—including its user anonymity, algorithmic recommendations of related groups, and the "push" e-mail notification of posts and responses—are content-neutral tools. *Roommates.Com*, 521 F.3d at 1168–69. They do not make Ultimate Software an "information content provider" 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," even if the tools were used to facilitate unlawful activities on the site. *See* 47 U.S.C. § 270(f)(3); *Roommates.com*, 521 F.3d at 1174 n.37; *Carafano*, 339 F.3d at 1123. In sum, Ultimate Software is immune

under § 230(c)(1) as a publisher of content created entirely by third-party users.

1.2.3.2 Online Market For Drug Trafficking and Shielding Bad Actors

Ms. Dyroff contends Ultimate Software knew or should have known that users sold drugs on Experience Project, and it shielded bad actors from the consequences of the drug dealing through its anonymity policies and antipathy to law-enforcement requests.[50] The idea is that Ultimate Software is less Match.com and more Silk Road (a notorious online platform for criminal activities, including selling illegal drugs). As evidence of Ultimate Software's intent to shield bad actors from law-enforcement efforts, the complaint cites Ultimate Software's March 2016 public statement discussing its reasons for suspending the Experience Project website.

> From day one, the privacy of our users has been paramount and we have never allowed names, phone numbers, or addresses. This approach bucked every trend, and challenged our ability to build an advertising-based business, but we passionately believe it provided the foundation for some of the most meaningful relationships imaginable . . . But there is no denying that the way people expect to use social media today is markedly different . . . and as the primary use has moved from web

---

[50] *Id.* at 18; *see also* Compl.—ECF No. 1-1 at 17–19 (¶¶ 39–42).

> to mobile, our hallmark attributes like long-form stories are not aligned.
>
> But, there are deeper, and more troubling trends than formats. Online anonymity, a core part of EP, is being challenged like never before. Governments and their agencies are aggressively attacking the foundations of internet privacy with a deluge of information requests, subpoenas, and warrants. We, of course, always support proper law enforcement efforts, but the well-documented potential for even abuse, even if unintentional, is enormous and growing.[51]

The complaint's allegations do not establish a theory of liability. The statement manifests a concern with Internet privacy that has been widespread in the technology sector and does not establish antipathy to law enforcement, especially given the statement about supporting "proper law enforcement requests."

Moreover, as the analysis in the last section establishes, Ultimate Software's functionalities are neutral tools that do not transform Ultimate Software into an "information content provider," even if the tools were used to facilitate unlawful activities on the site. 47 U.S.C. § 270(f)(3); *Roommates.com*, 521 F.3d at 1174 n.37; *Barnes*, 570 F.3d at 1103; *Gonzalez*, 2017 WL 4773366, at *10. Ultimate Software's policy about anonymity may have allowed illegal conduct, and the neutral tools facilitated user communications, but these website functionalities do not "create" or "develop"

---

[51] Compl.—ECF No. 1-1 at 17–18 (¶ 41) (emphasis omitted).

information, even in part. 47 U.S.C. § 270(f)(3); *Roommates.com*, 521 F.3d at 1174 n.37; *Carafano*, 339 F.3d at 1123. And they do not show that Ultimate Software engaged in "substantial affirmative conduct . . . promoting the use of [the] tools for unlawful purposes." *Roommates.com*, 521 F.3d at 1167–68, 1174 n.37. Liability requires more than "neutral tools." *Id.*

As the Ninth Circuit concluded in *Roommates.com*: "

> Websites are complicated enterprises, and there will always be close cases where a clever lawyer could argue that something the website operator did encouraged the illegality. Such close cases, we believe, must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to . . . fight[] off claims that they promoted or encouraged—or at least tacitly assented to—the illegality of third parties. Where it is very clear that the website directly participates in developing the alleged illegality . . . [,] immunity will be lost. But in cases of enhancement by implication or development by inference . . . [,] section 230 must be interpreted to protect websites not merely from ultimate liability, but from having to fight costly and protracted legal battles.

521 F.3d at 1174–75.

Because Ultimate Software is immune under § 230(c)(1), the court dismisses all claims except claim four.

2. Count Four: Failure to Warn

In claim four, Ms. Dyroff contends that Ultimate Software had a duty to warn Mr. Greer that Mr. Margenat-Castro was selling fentanyl-laced heroin via the Experience Project website.[52] Ultimate Software moves to dismiss the claim on the grounds that (1) it had no "special relationship" with Mr. Greer or created any risks that gave rise to a duty to warn him, and (2) Mr. Greer assumed the risk of buying drugs from an anonymous Internet drug dealer.[53] The CDA does not preclude a failure-to-warn claim. *Internet Brands*, 824 F.3d at 849–54.

The next sections address (1) whether Ultimate Software had a "special relationship" with Mr. Greer that gave rise to a duty to warn, (2) whether Ultimate Software created a risk that gave rise to a duty to warn, and (3) whether the assumption-of-risk doctrine bars recovery.

2.1 Duty to Warn: Special Relationship—Nonfeasance (Failure to Act)

The first issue is whether Ultimate Software had a duty to warn Mr. Greer that Mr. Margenat-Castro was selling fentanyl-laced heroin because—like any brick-and-mortar business—it had a "special relationship" with him that created that duty.

---

[52] Motion to Dismiss—ECF No. 13-1 at 18–21; Reply—ECF No. 16 at 18–20.

[53] *Id.*

The California Supreme Court has not addressed whether a website has a special relationship with its users that gives rise to a duty to warn them of dangers. The court's task thus is to "predict how the state high court would resolve" the issue. *Giles v. Gen. Motors Acceptance Corp.*, 494 F.3d 865, 872 (9th Cir. 2007) (quotation omitted). For guidance, the court looks to decisions in the state's intermediate appellate courts and other jurisdictions. *Id.*

The elements of a negligence claim are (1) the existence of a duty to exercise due care, (2) breach of that duty, (3) causation, and (4) damages. *Merrill v. Navegar, Inc.*, 28 P.3d 116, 139 (Cal. 2001). A duty to exercise due care is an "obligation to conform to a certain standard of conduct for the protection of others against unreasonable risks." *McGarry v. Sax*, 158 Cal. App. 4th 983, 994 (2008) (quotation omitted).

"'The existence of a legal duty to use reasonable care in a particular factual situation is a question of law for the court to decide.'" *McGarry*, 158 Cal. App. 4th at 994 (quoting *Adams v. City of Fremont*, 68 Cal. App. 4th 243, 265 (1998)); *Thompson v. County of Alameda*, 27 P.2d 728, 732 (Cal. 1980); *Vasquez*, 118 Cal. App. 4th 269, 279 (2004) (Imposing a duty is "'an expression of policy considerations leading to the legal conclusion that a plaintiff is entitled to a defendant's protection.'") (quoting *Ludwig v. City of San Diego*, 65 Cal. App. 4th 1105, 1110 (1998)); *accord Tarasoff v. Regents of Univ. of California*, 551 P.2d 334, 342 (Cal. 1976) ("legal duties are not discoverable facts of nature, but merely conclusory expressions that, in cases

of a particular type, liability should be imposed for damage done").

Under California law, if a person has not created a danger, then generally he has no duty to come to the aid of another person (a victim) absent a relationship that gives rise to a duty to protect. *Zelig v. County of Los Angeles*, 45 P.3d 1171, 1182 (Cal. 2002); *accord McGarry*, 158 Cal. App. 4th at 995. The "special relationship" can be between the person and a third party that imposes a duty to control the third party's conduct. *Zelig*, 45 P.3d at 1183. Or it can be a special relationship between the person and the foreseeable victim of the third party's conduct that requires the person to protect the victim. *Id.*; *accord Tarasoff*, 551 P.2d at 342.

The "special relationship" giving rise to a duty to protect derives "from the common law's distinction between misfeasance and nonfeasance, and its reluctance to impose liability for the latter." *Zelig*, 45 P.3d at 1183 (quotation omitted). Nonfeasance is a failure to act. *Weirum v. RKO Gen., Inc.*, 539 P.2d 36, 41 (Cal. 1975). "Misfeasance exists when the defendant is responsible for making the plaintiff's position worse, i.e., defendant has created a risk." *Id.* With misfeasance, the question of duty is governed by the ordinary-care standard for negligence. *Lugtu v. California Highway Patrol*, 26 Cal. 4th 703, 716 (2001).

In sum, a "special relationship" can create a duty to act even when one otherwise would not have such a duty. *Zelig*, 45 P.3d at 1183. Ultimate Software thus can be responsible for its nonfeasance (its failure to

act) if (1) it had a special relationship with a third-party actor and thus had a duty to control that actor, or (2) it had a special relationship with Mr. Greer and thus owed him a duty to protect him. *Id.* The plaintiff argues that like any business, Ultimate Software has a "special relationship" with its customers that creates a duty to warn them of known risks.[54]

Courts commonly involve the special-relationship doctrine "'in cases involving the relationship between business proprietors such as [landlords,] shopping centers, restaurants, and bars, and their tenants, patrons, or invitees.'" *McGarry*, 158 Cal. App. 4th at 995 (quoting *Delgado v. Trax Bar & Grill*, 113 P.3d 1159, 1165 (Cal. 2005)). "A business owner may have an affirmative duty to 'control the wrongful acts of third persons which threaten invitees where the [business owner] has reasonable cause to anticipate such acts and the probability of injury resulting therefrom.'" *Id.* (citing *Taylor v. Centennial Bowl, Inc.*, 416 P.2d 793 (1966)). "The doctrine also extends to other types of special relationship[s] . . . including those between common carriers and passengers, and mental health professionals and their patients." *Id.* (quoting *Tarasoff*, 551 P.2d at 334). These "special relationships generally involve some kind of dependency or reliance." *Olson v. Children's Home Soc'y*, 204 Cal. App. 3d 1362, 1366 (1988); *see e.g.*, *Williams v. State of California*, 664 P.2d 137, 139 (Cal. 1983) (a factor supporting a special relationship is detrimental reliance by a person on another

---

[54] Motion to Dismiss—ECF No. 15 at 26.

person's conduct that induced a false sense of security and worsened the position of the person relying on the conduct).

"'[T]he use of special relationships to create duties has been largely eclipsed by the more modern use of balancing policy factors enumerated in *Rowland* [*v. Christian.*]'" *McGarry*, 158 Cal. App. 4th at 996 (quoting *Doe 1 v. City of Murrieta*, 102 Cal. App. 4th 899, 918 (2002)) (citing *Rowland v. Christian*, 443 P.2d 561, 564 (Cal. 1968)). The *Rowland* factors are the following: "[(1)] the foreseeability of harm to the plaintiff, [(2)] the degree of certainty that the plaintiff suffered injury, [(3)] the closeness of the connection between the defendant's conduct and the injury suffered, [(4)] the moral blame attached to the defendant's conduct, [(5)] the policy of preventing future harm, [(6)] the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach, and [(7)] the availability, cost, and prevalence of insurance for the risk involved." *Id.* at 996–97 (quoting *Rowland*, 443 P.2d at 564); *see also Hansra v. Superior Court*, 7 Cal App. 4th 630, 646 (1992) ("whether a special relationship exists giving rise to a duty to protect . . . [involves] consideration of the same factors underlying any duty of care analysis").

Following remand of the *Internet Brands* case, the district court addressed whether a website has a "special relationship" with its users that required the website to warn users of known risks on the website. *See Jane Doe No. 14 v. Internet Brands, Inc.*, No.

2:12-CV-3626-JFW (PJW), ECF No. 51 (C.D. Cal. Nov. 14, 2016). The court found no special relationship and thus no duty to warn. *Id.* at 5–6.

The plaintiff was an aspiring model who was a member of the networking website modelmayhem.com. *Id.* at 1. Two men—who were unaffiliated with the website—used the website to identify and lure victims (including the plaintiff) to Florida, where they drugged and raped the victims, filming the rapes for distribution as pornography videos. *Id.* at 2. The plaintiff claimed that by the time she was raped in 2011, Internet Brands knew about the two men, had a duty to warn its users, and thus was liable for its negligent failure to warn her. *Id.* at 2–3.

The case involved nonfeasance, not misfeasance. *Id.* at 5 (rejecting as unsubstantiated the claim that Internet Brands created the risk). The court found no "special relationship" between Internet Brands and the two men who carried out the rape scheme, and it thus found that Internet Brands had no duty to control their conduct. *Id.* It then addressed whether Internet Brands had a "special relationship" with the victim-plaintiff, who was a member of the website "along with at least 600,000 others." *Id.* The court applied the *Rowland* factors and concluded that there was no special relationship between the website and its users and thus no duty to warn. *Id.* at 5–6.

Another district court—again on remand from the Ninth Circuit—also concluded that a website had no duty to warn its users. *Beckman v. Match.com, LLC*,

No. 2:13-CV-97 JCM (NJK), 2017 WL 1304288, at *4 (D. Nev. Mar. 10, 2017). The plaintiff met and dated a man on Match.com and ended their relationship eight days later. *Id.* at *1. He then sent her threatening messages for about four days, and four months later, attacked her viciously. *Id.* She sued Match.com for failure to warn her that the website and her attacker were dangerous, basing her claim in part on Match.com's access to data about its users and use of the data to create matches. *Id.* at *1–*3. Applying Nevada law, which is similar to California law, the court found no special relationship between Match.com and the plaintiff. *Id.* at *3–*4. The plaintiff was merely a paying subscriber, paid the fee, set up her profile, and was matched with the attacker. *Id.* at *3. The court concluded that the website had no special relationship with the plaintiff and thus no duty to warn her. *Id.* at *4.

These cases support the conclusion that a website has no "special relationship" with its users. Ms. Dyroff nonetheless contends that websites [sic] operators such as Ultimate Software are the "twenty-first century equivalent of a brick and mortar business . . . like restaurants, bars, . . . amusement parks, and all businesses open to the public" and have the same duty that all businesses open to the public owe their invitees. The duty "includ[es] 'tak[ing] affirmative action to control the wrongful acts of third persons which threaten invitees where the occupant has reasonable cause to

anticipate such acts and the probability of injury resulting therefrom."[55]

If the court followed this approach, it would render all social-network websites potentially liable whenever they connect their members by algorithm, merely because the member is a member. This makes no sense practically. Imposing a duty at best would result in a weak and ineffective general warning to all users. *Internet Brands*, No. 2:12-cv-3626-JFW (PJW), ECF No. 51 at 6. It also "likely [would] have a 'chilling effect' on the [I]nternet by opening the floodgates of litigation." *Id.* at 7 (referencing the briefs in the Ninth Circuit). Also, the court is not convinced that a bricks-and-mortar business (such as a bar where people meet more obviously) is a good analogue to a social-network website that fosters connections online. For one, allocating risk is (in part) about foreseeability of harm and the burdens of allocating risk to the defendant or the plaintiff. *See Rowland*, 443 P.2d at 561. Risk can be more apparent in the real world than in the virtual social-network world.[56] That seems relevant here, when

---

[55] Opposition to Motion to Dismiss—ECF No. 15 at 24–26 (quoting *Taylor v. Centennial Bowl, Inc.*, 416 P.2d 793, 797 (Cal. 1996)).

[56] Ms. Dyroff cites *eBay, Inc. v. Bidder's Edge, Inc.* to support the conclusion that a business's liability does not turn on the difference between a bricks-and-mortar business and an Internet business. Opposition to Motion to Dismiss—ECF No. 15 at 24–25 (citing 100 F. Supp. 2d 1058, 1065 (N.D. Cal. 2000)). *eBay* does not change the court's conclusion. In *eBay*, the court granted eBay a preliminary injunction to prevent a competing auction website from scanning eBay's website for auction information. 100 F. Supp. 2d at 1065. The court held that the difference between

the claim is that a social-network website ought to perceive risks—through its automatic algorithms and other inputs—about a drug dealer on its site.

Moreover, even if Ultimate Software had superior knowledge about Mr. Margenat-Castro's selling fentanyl-laced heroin, that knowledge does not create a special relationship absent dependency or detrimental reliance by its users, including Mr. Greer. *Internet Brands*, No. 2:12-cv-3626-JFW (PJW), ECF No. 51 at 6 ("it may have been foreseeable that [the two men] would strike again"). For example, in *Conti v. Watchtower Bible & Tract Society of New York, Inc.*, the California Court of Appeal held that a religious organization had no special relationship with its congregation and thus had no duty to warn them—despite its knowledge of the high risk of recidivism—that a fellow member was a child molester. *Id.* (citing *Conti*, 235 Cal. App. 4th 1214 (2015), as the case with the most analogous facts). In *Olson*, the California Court of Appeal held that there was no ongoing "special relationship" between an adoption agency and a birth mother who gave up her son for adoption that required the agency to notify the birth mother when it learned that the son tested positive for a serious inherited disease passed

---

eBay's virtual store and a physical store were "formalistic," and it found the competitor's actions more like a trespass to real property (as opposed to a trespass to chattels) because the electronic signals were sufficiently tangible to equate to a physical presence on eBay's property. *Id.* at 1067 & n.16. That result makes sense: there was a threatened physical incursion onto eBay's website. But it provides no support for equating bricks-and-mortar businesses (such as bars) to social-network websites.

from mothers to their male offspring. *Olson*, 204 Cal. App. 3d at 1366–67. The birth mother later had a second son with the same affliction. *Id.* By contrast, a duty can arise for a defendant with superior knowledge if there is dependency or reliance. *See Internet Brands*, No. 2:12-cv-3626-JFW (PJW), ECF No. 51 at 6 n.3 (citing *O'Hara v. Western Seven Trees Corp.*, 75 Cal. App. 3d 798 (1977)). In *O'Hara*, the landlord had a duty to warn his tenant, who was raped, about the risks because he knew of prior rapes at the apartment complex, knew about the likelihood of a repeat attack because police gave him composite drawings of the suspect and a description of his modus operandi, failed to warn his tenant, and assured her that the premises were safe and patrolled at all times by professional guards). *Id.* (citing *O'Hara*, 75 Cal. App. 3d 798). Here, Ms. Dyroff has not alleged dependency or reliance.

In sum, the court holds that there was no special relationship between Ultimate Software and Mr. Greer that gave rise to a duty to warn.

2.2 Duty to Warn—Misfeasance (Creation of Risk)

Ms. Dyroff also contends that Ultimate Software created a risk of harm through its website functionalities and thus owed her son an ordinary duty of care to warn him about Mr. Margenat-Castro's trafficking of fentanyl-laced heroin.[57] The court holds that Ultimate Software's use of the neutral tools and functionalities

[57] Opposition to Motion to Dismiss—ECF No. 15 at 26.

on its website did not create a risk of harm that imposes an ordinary duty of care. *See Lugtu*, 28 P.3d at 256–57 (negligence standard for misfeasance). A contrary holding would impose liability on a social-network website for using the ordinary tools of recommendations and alerts. The result does not change merely because Experience Project permitted anonymous users.

2.3 Assumption of Risk

The last issue is whether the assumption-of-risk doctrine bars Mr. Greer's failure-to-warn claim. Because the court holds that there is no duty to warn, it does not reach the issue. If it were to reach the issue, it would likely hold that the doctrine operates as a complete bar to his claim because Mr. Greer—who initiated the contact with Mr. Margenat-Castro by his posts on Experience Project and then bought drugs from him—assumed the obviously dangerous risk of buying drugs from an anonymous Internet drug dealer. *See, e.g.*, *Souza v. Squaw Valley Ski Corp.*, 138 Cal. App. 4th 262, 266–67 (2006).

* * *

CONCLUSION

The court grants the motion to dismiss without prejudice. The plaintiff must file any amended complaint within 21 days.

This disposes of ECF No. 13.

IT IS SO ORDERED.

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

Effective: April 11, 2018

(a) Findings

The Congress finds the following:

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

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

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

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

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

(b) Policy

It is the policy of the United States –

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

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

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

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

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

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

(1) Treatment of publisher or speaker

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

(2) Civil liability

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

> **(A)** any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> **(B)** any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[1]

(d) Obligations of interactive computer service

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

---

[1] So in original. Probably should be "subparagraph (A)".

(e) Effect on other laws

(1) No effect on criminal law

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

(2) No effect on intellectual property law

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

(3) State law

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

(4) No effect on communications privacy law

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

(5) No effect on sex trafficking law

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

(A) any claim in a civil action brought under section 1595 of Title 18, if the conduct

underlying the claim constitutes a violation of section 1591 of that title;

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

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

(f) Definitions

As used in this section:

(1) Internet

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

(2) Interactive computer service

The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

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

(4) Access software provider

The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.