No. 18-15175

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

KRISTANALEA DYROFF,

Plaintiff-Appellant,

v.

THE ULTIMATE SOFTWARE GROUP, INC.

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
No. 3:17-cv-05359-LB

THE HONORABLE LAUREL BEELER

APPELLANT'S OPENING BRIEF
ORAL ARGUMENT REQUESTED

Sin-Ting Mary Liu
Aylstock, Witkin, Kreis & Overholtz, PLLC
875-A Island Drive #144
Alameda, CA 94502
(510) 698-9566 Telephone
(760) 304-8933 Facsimile
mliu@awkolaw.com

David Slade
Carney Bates & Pulliam, PLLC
519 W. 7th St.
Little Rock, AR 72201
(501) 312-85500 Telephone
(501) 312-8505 Facsimile
dslade@cbplaw.com

Counsel for Plaintiff-Appellant, Kristanalea Dyroff

CORPORATE DISCLOSURE STATEMENT

Pursuant to the disclosure requirements of FRAP 26.1, Kristanalea Dyroff declares that she is an individual, and is not a subsidiary or affiliate of a publicly owned corporation and there is no publicly held corporation that owns ten percent or more of any stock issued by her.

Dated: June 13, 2018

Respectfully submitted,

/s/ David Slade

David Slade
Carney Bates & Pulliam, PLLC
519 W. 7th St.
Little Rock, AR 72201
Phone: 501-312-8500
Fax: 501-312-8505

Sin-Ting Mary Liu
Aylstock, Witkin, Kreis, & Overholtz, PLLC
875-A Island Drive #144
Alameda, CA 94502
mliu@awkolaw.com
Phone: 510-698-9566
Fax: 760-304-8933

Attorneys for Plaintiff-Appellant, Kristanalea Dyroff

STATEMENT REGARDING ORAL ARGUMENT

Oral argument would assist the Court in evaluating this appeal. Plaintiff-Appellant requests that each side be allotted a minimum of 30 minutes for oral argument, with Plaintiff-Appellant permitted to divide that time between opening argument and rebuttal at her discretion.

Dated: June 13, 2018

Respectfully submitted,

/s/ David Slade
David Slade
Carney Bates & Pulliam, PLLC
519 W. 7th St.
Little Rock, AR 72201
Phone: 501-312-8500
Fax: 501-312-8505

Sin-Ting Mary Liu
Aylstock, Witkin, Kreis, & Overholtz, PLLC
875-A Island Drive #144
Alameda, CA 94502
mliu@awkolaw.com
Phone: 510-698-9566
Fax: 760-304-8933

Attorneys for Plaintiff-Appellant, Kristanalea Dyroff

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases **Page**

Rules and Statutes

I. STATEMENT OF JURISDICTION

The district court had subject matter jurisdiction pursuant to 28 U.S.C. § 1332(a).

On November 26, 2017, the district court dismissed all claims against Defendant with leave to amend. ER2-ER27.[1] On January 19, 2018, Plaintiff Kristanalea Dyroff filed a Notice of Intent Not to File an Amended Complaint. CD31. On that same day, the district court entered judgement in favor of Defendant and against Plaintiff, pursuant to Federal Rule of Civil Procedure 58. ER1. The dismissal and order of judgment gave this Court jurisdiction under 28 U.S.C. § 1291.

Plaintiff timely appealed on February 2, 2018. ER28-ER31.

II. ISSUES PRESENTED

1. Defendant designed its website to identify the meaning of, and intent behind, its users' posts. Defendant used that information to infer characteristics about those users and to pair them with other users who shared related characteristics. Defendant used this functionality to identify Wesley Greer as a heroin addict, and to steer him to posts made by heroin dealers on its website. Did the district court err in holding that Defendant's promotion of posts involving the

[1] "ER__" denotes the Excerpts of Record, while "CD__" denotes numbered entries in the district court clerk's docket.

sale of heroin did not make it responsible, in whole or in part, for the creation or development of information related to those posts?

2. The CEO of Defendant's website publicly stated that he had elected to shut the website down in order to avoid law enforcement requests related to unlawful user activity. Did the district court err in holding that this statement, along with Defendant's anonymity policy for its users, did not make it responsible, in whole or in part, for the creation or development of information related to unlawful posts that it fostered on its website?

3. Defendant's website identified Wesley Greer as a heroin addict and steered him towards posts advertising the sale of heroin. Among those were posts from Hugo Margenat-Castro, a man Defendant knew to be under investigation for selling fentanyl and who had been arrested several times for having done so. With this knowledge, Defendant identified Wesley Greer as a heroin addict and purposely directed him to Margenat-Castro, from whom Mr. Greer purchased a fatal dose of fentanyl, advertised as heroin. Did the district court err in holding that Defendant's misfeasance did not create a risk to Mr. Greer and therefore that it owed him no duty of care?

4. Did the district court err in holding that Defendant owed no duty of care to Wesley Greer as an invitee?

III. STANDARD OF REVIEW

This Court reviews *de novo* a complaint's dismissal under Federal Rule of Civil Procedure 12(b)(6). *Stearns v. Ticketmaster Corp*., 655 F.3d 1013, 1018 (9th Cir. 2011). "Dismissal is proper only where there is no cognizable legal theory or an absence of sufficient facts alleged to support a cognizable legal theory." *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). To survive a motion to dismiss, the complaint must allege "enough facts to state a claim to relief that is plausible on its face." *Taylor v. Yee*, 780 F.3d 928, 935 (9th Cir. 2015) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007)). "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." *Ashcroft v. Iqball*, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009) (quoting *Twombly*, 550 U.S. at 557). 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) (citation and quotation omitted).

IV. STATEMENT OF THE CASE

A. Introduction

Plaintiff Kristanalea Dyroff seeks to hold Defendant[2] liable for its role in the death of her son, Wesley Greer. Until shutting down in March 2016, Defendant's social network website was a haven for drug traffickers and, correspondingly, a peril for vulnerable addicts. Defendant did not serve as a passive conduit for the drug sales. Instead, it contributed to these unlawful enterprises in multiple, material ways.

First, through its recommendations functionality—which drew on Defendant's specific knowledge of its users, obtained via algorithms, data mining technology, and inferences drawn from the demographic characteristics—Defendant identified vulnerable addicts and steered them through an echo chamber, pushing those users into continued contact with dealers through groups with names such as "I Need Heroin" and "I Can Help With Connect in Orlando FL." Defendant also

[2] Plaintiff filed this action against the following entities: Experience Project, Kanjoya, Inc. ("Kanjoya"), and Ultimate Software Group, Inc. ("Ultimate Software Group"). ER32-ER88. Ultimate Software Group purchased all of the interests in Experience Project from Kanjoya in 2016, and Kanjoya was subsequently merged with Ultimate Software Group. Because Ultimate Software Group is the only one of the three entities currently in existence, Plaintiff dismissed her claims against Experience Project and Kanjoya in the underlying litigation without prejudice. CD18. Although Ultimate Software Group is the Defendant, the acts and practices detailed herein arise from Experience Project. Accordingly, Plaintiff refers to all three entities as either "Experience Project" or "Defendant."

oversaw a messaging functionality that would connect addicts with dealers and would alert addicts to new posts in groups related to the sale of drugs.

Second, Defendant's content generation guidelines were developed to assure anonymity of users, which fact was seized upon by dealers. This decision was not neutral—Defendant publicly stated that it sought to preserve online anonymity of its users, at least in part, to combat law enforcement investigations and requests for information. Indeed, once those requests for information became voluminous (given the ubiquity of criminal activity on Defendant's website), Defendant shuttered the site rather than aid any investigations.

Plaintiff's son was a victim of the environment created and maintained by Defendant. In August of 2015, Wesley, a recovering heroin addict, established an account with Defendant's website and, like other vulnerable users, was steered towards multiple groups devoted to the sale of heroin. Subsequently, he was steered towards a man named Hugo Margenat-Castro, from whom he purchased what he believed to be heroin, but what was in reality fentanyl, a lethal substance 50 times more potent than heroin. That lack of knowledge led to Wesley's overdose and death on August 19, 2015. While Wesley did not know that Margenat-Castro sold fentanyl, Defendant *did* know or should have known. Margenat-Castro was the subject of multiple controlled buys and arrests from various law enforcement agencies throughout 2015, and the investigations surrounding those arrests led

authorities to Defendant's website, and led to numerous requests from law enforcement related to Margenat-Castro. Therefore, prior to Wesley's death, Defendant knew or should have known not only that Margenat-Castro was trafficking drugs on Experience Project, but that he was trafficking *fentanyl*. Had Defendant warned Wesley of this fact, he would not have overdosed and died.

B. Factual Background

i. The Experience Project Website

Experience Project was a social networking website active from 2007 until March 2016. ER38:¶18. The website consisted of various "online communities" or "groups" that were formed by members based on common interests or attributes. *Id*. Users were required to register with the site in order to join these communities or groups, but per the website's policy they did so anonymously. ER38:¶19, ER46:¶36-ER48:¶42. Once a user joined a group, he or she could post questions or comments to that group or respond to another user's comments or questions. ER39:¶21.

This user interaction generated revenue for Experience Project in several ways. ER39:¶22. First, the website served ads to its users. *Id*. Second, users could buy "tokens" that they could then use to ask other members questions. ER41:¶25. Third, the website used data mining techniques, including the use of machine learning models, to analyze its users' posts, divining the content (by "assessing entire sentence structures") as well as the underlying emotions associated with the posts.

ER39:¶22, ER40:¶23. Defendant used the information created from that data mining for several purposes, including selling the data sets to various third parties (ER39-ER40:¶22, citing http://www.frbsf.org/economic-research/files/wp2017-01.pdf), but also using what it learned about its users to steer them to *other* groups, in order to keep them engaged on the site (ER41:¶27-ER42:¶28). Experience Project would identify these additional groups and tailor them to individual users through its recommendations functionality. *Id.* This recommendations functionality would take data that Experience Project gleaned from its users—including the content of a given group, the content posted by users within the group, the demographic data known by Experience Project about a given user (including geographic location)—and would then compile that data and draw inferences from that compilation about what other interactions a user might seek on the website. *Id.* All of these data points were derived, bundled, maintained, and used for Defendant's commercial gain. *Id.*

In part because of its opportunity for anonymous-yet-public dialogue, Experience Project became a popular medium for drug dealers and drug addicts. ER41:¶26-ER45:¶35, ER47:¶41-ER48:¶42. Defendant did not sit idly by as these two demographic groups sought each other out. Instead, through its recommendations functionality, Defendant first identified and the tempted vulnerable drug addicts with continual entreaties to connect with drug dealers, thus encouraging further interactions (and valuable data generated therefrom) through the

website's feedback loop. ER41:¶26-ER45:¶35 Among the drugs that were trafficked on the website were heroin and other opiates. ER42:¶30.

Experience Project facilitated this activity with full knowledge. It was aware of the dangerous and unlawful sale of drugs on its property, both through the data it acquired and utilized in the course of its mining and manipulation of users' posts (ER46:¶38) and as the result of myriad requests for information from law enforcement, which arose from separate criminal investigations and/or prosecutions related to the illegal activity perpetrated on the website. ER47:¶39-ER48:¶42, ER54:¶65-¶68, ER56:¶71, ER56:¶73, ER54:n.13. Concerning the latter, eventually the requests from law enforcement became too much, and Experience Project elected to shut the website down rather than aid investigations into criminal activity. ER47:¶39-ER48:¶42. On March 21, 2016, the website posted an open letter to its users, stating that a "deep[]" and "troubling trend[]" threatened the website; specifically, "[o]nline 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." ER47:¶41. Accordingly, the website announced that it would be "taking a break." *Id*.

ii. The Death of Wesley Greer

Wesley Greer was a recovering heroin addict, having become addicted to the drug following an over-prescription of opiates after a sports injury in college. ER49:¶44-¶48. After multiple attempts at rehabilitation, Wesley had managed to stay clean beginning in August, 2013, following a 9-month stay at a treatment facility. ER49:¶46. In February, 2015, Wesley moved to Brunswick, Georgia, with his mother and stepfather who wanted to support Wesley in his recovery. ER49:¶48. However, in August 2015, Wesley succumbed, conducting a web search to find heroin that led him to the Experience Project site. ER50:¶49. He then registered for an account, paid for tokens to ask questions of other users, and began posting to groups related to the sale of heroin. ER50:¶49-¶50. Subsequently, through Experience Project's messaging functionality, the website directly alerted Wesley to new posts in these groups. ER50:¶52.

At or around this time, a fellow Experience Project user, Hugo Margenat-Castro, had been posting in multiple groups under the alias "Potheadjuice," purporting to sell heroin. In reality, Margenat-Castro was selling fentanyl, a synthetic opioid that is 50 times more potent than heroin and is a substance so toxic that a dose the size of three grains of sugar is fatal to an adult. ER50:¶53-¶54, ER51:¶58. Margenat-Castro sold pure fentanyl and/or heroin laced with fentanyl, used Experience Project as his exclusive vehicle for drug sales, and availed himself

not only of its anonymity policy and content guideline, but also of its recommendations and messaging functionality, as well as its antipathy towards requests for information from law enforcement about criminal activity on the site. ER52:¶59. Margenat-Castro sold drugs five sales a day, seven days a week, from January 1, 2015 until October 1, 2015. ER51:¶58, ER52:¶60, ER52:n.11, ER52:n.12. He did this exclusively through Experience Project, which is corroborated by an almost 1:1 ratio of profile views to drug sales. ER52:¶60, ER52:n.11, ER52:n.12.

Since January, 2015, multiple law enforcement agencies had targeted Margenat-Castro for his drug trafficking on Experience Project, conducting controlled buys and effecting subsequent arrests multiple times in the Spring and Summer of 2015. ER51:¶61. In the course of these investigations during this time period, Experience Project would or should have had actual knowledge of Margenat-Castro's illegal activities on the website—including the fact that he was selling fentanyl despite his representations that he was simply selling heroin. ER54:¶65-¶66, ER54:n.13.

On or about the night of August 17, 2015, Wesley made contact with Margenat-Castro, via Experience Project, and arranged to buy what he believed to be heroin. ER50:¶55. In reality, he had purchased a lethal dose of fentanyl. *Id.* On the evening of August 18, 2015, Wesley ingested the drugs he had purchased.

ER51:¶56. By August 19, 2015, at 11:55 A.M., Wesley was declared dead of fentanyl toxicity; his death was listed as a homicide. ER51:¶57.

A. Procedural History

Plaintiff Kristanalea Dyroff, individually and on behalf of her son's estate, filed a lawsuit against Defendants Ultimate Software Group, Experience Project, and Kanjoya, Inc. in California Superior Court on August 16, 2017. ER32-ER88. Her complaint advanced seven claims: negligence (Count One), wrongful death (Count Two), premises liability (Count Three), failure to warn (Count Four), civil conspiracy (Count Five), unjust enrichment (Count Six), and violation of the Drug Dealer Liability Act, Cal. Health and Safety Code §§ 11700, *et seq.* (Count Seven). ER56-ER67 Subsequently, Defendant Ultimate Software Group filed a Notice of Removal on September 15, 2017. CD1. Shortly thereafter, Defendant Ultimate Software Group moved to dismiss the Complaint (CD13); Plaintiff opposed (CD15); and Defendant filed its reply (CD16). The district court heard oral argument on November 2, 2017 (CD20), and on November 26, 2017 it issued an order granting Defendant's motion to dismiss and allowing Plaintiff leave to amend (ER2-ER27).

Plaintiff timely appealed on February 2, 2018. ER28-ER31.

B. The Ruling Below

For all of Plaintiff's claims except for her failure to warn claim, the district court held that Defendant was entitled to immunity under Section 230 of the

Communications Decency Act, 47 U.S.C. § 230 ("Section 230"). ER3. In the court's view, Plaintiff's claims sought to hold Defendant (a website) liable for content posted by third parties, which is precluded by Section 230. ER3. Although Plaintiff asserted that her claims did not arise from third-party content, but rather from specific behavior and functionality on the part of the website,[3] the court disagreed, finding that "only third parties posted information on Experience Project, and the website operator did not solicit unlawful information or otherwise create or develop content." ER16.

The district court also rejected Plaintiff's argument that Defendant's policies and procedures knowingly sanctioned, aided, and abetted the illegal activity on its website, thereby helping "develop" the content and precluding Section 230 immunity. ER18-ER20. Although Plaintiff provided a statement from the website's founder announcing that he was shuttering the site because of "troubling trends" related to law enforcement interest in the website and its users' illegal activity, resulting in "a deluge of information requests, subpoenas, and warrants," the court held that this was not a sufficient indicium that the website condoned and enabled

[3] As the district court correctly summarized, Plaintiff alleged that Experience Project "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." ER15. Plaintiff challenged these acts and practices, which "'created an environment where vulnerable addicts were subjected to a feedback loop of continual entreaties to connect with drug dealers.'" *Id.*

its users' bad acts. ER19. The court reached a different inference, finding "[t]he statement manifest[ed] a concern with Internet privacy…and does not establish antipathy to law enforcement." *Id*. The website's "policy about anonymity may have allowed illegal conduct," the court held, but ultimately neither the policy nor the "neutral tools [that] facilitated user communications" could be said to "'create' or 'develop' information, even in part." *Id*. Accordingly, in the court's view, Section 230 foreclosed all of Plaintiff's claims save for her failure to warn claim.

The district court dismissed Plaintiff's failure to warn claim[4] on the grounds that no duty was owed to Wesley Greer by Defendant, either because of a special relationship between the parties or because of the website's role in creating the risks that gave rise to his overdose and homicide. ER20-ER26. Concerning the former point, the court rejected Plaintiff's argument that social media websites "are 'the twenty-first century equivalent of a brick and mortar business…like restaurants, bars,…amusement parks, and all businesses open to the public,'" holding that "[t]his makes no sense practically. Imposing a duty at best would result in a weak and ineffective general warning to all users." ER24. Further, imposing a duty of care would be inappropriate as "[r]isk can be more apparent in the real world than in the virtual social-network world." ER25. Concerning a duty imposed as a result of the

[4] As stated by the district court, Plaintiff contended that Defendant "had a duty to warn Mr. Greer that Mr. Margenat-Castro was selling fentanyl-laced heroin via the Experience Project website." ER20.

website's pushing drug addicts to engage with drug dealers (i.e., its misfeasance), the court held that Defendant's "use of the neutral tools and functionalities on its website did not create a risk of harm that imposes an ordinary duty of care." ER26.

The court dismissed all claims with leave to amend. ER27.

V. SUMMARY OF ARGUMENT

The district court erred in three respects.

First, it mischaracterized Experience Project's recommendations functionality and push notifications—which in the instant matter identified a vulnerable heroin addict and relentlessly steered him to a known drug trafficker—as "content-neutral tools" worthy of Section 230 Immunity. Instead, Plaintiff's allegations demonstrate that the website was specifically designed to make subjective, editorial decisions about users based on their posts. Although the website could classify users in benign categories (e.g., "I'm going to Stanford") it also was able to (and did) identify and categorize users according to characteristics that were both unlawful and, more importantly, profoundly harmful to those grouped individuals. This conduct was particularly dangerous—and far from neutral—because Experience Project would *then* steer the users it identified as heroin addicts to users it had identified as heroin *dealers*, thereby facilitating a drug deal.

It cannot be overstated that the Defendant professed to know exactly what each of its users were posting and what the intent was behind each post. The conduct

Plaintiff challenged is therefore not a neutral action wholly reliant on third-party inputs, but instead the product of a series of knowing, deliberate acts, unlawfully and *independently* undertaken by Defendant and Defendant, alone. Indeed, neither the drug-trafficker user nor the drug-addict user had any control over the functionality challenged by Plaintiff; Margenat-Castro could not have steered Wesley Greer to his posts even if he tried. The agency lay exclusively with Defendant. Under controlling Ninth Circuit authority, such deliberate acts are not subject to Section 230 immunity, and instead clearly evidence the development, on the part of the website, of its own, harmful content.

Second, the district court erred in refusing to credit Plaintiff's well-pleaded allegations that Experience Project not only knew of the activity occurring on the website, but condoned the bad acts and even *colluded* with the bad actors using the site, through its posting policies and through its stated antipathy towards law enforcement. Although the district court was presented with a public statement by Experience Project's CEO that he was shuttering the website due to a "deluge of information requests, subpoenas, and warrants" (rather than aid authorities), it declined to draw the entirely plausible and logical inference that such a statement indicated sympathy for users who were the subject of those requests (including Margenat-Castro) and antipathy towards law enforcement. Rather, and improperly, the district court explained this away as "a concern with Internet privacy that has

been widespread in the technology sector." This refusal to draw all inferences in Plaintiff's favor—particularly when courts have done so under nearly identical circumstances when applying this Court's law—is reversible error.

Third, the district court erred in finding that Defendant owed no duty to warn Wesley Greer of what it already knew from multiple, previous requests from law enforcement: that Margenat-Castro was trafficking not in heroin, but rather in pure fentanyl (a substance 50 times more deadly). This is incorrect for two reasons. First, under California law, a defendant owes a duty to warn of a danger created by his own misfeasance. The dangers endemic to Defendant's website were of Defendant's own making and were not the result of "neutral" tools, as the district court improperly held. Second, even if the risk did not arise from Defendant's misfeasance, it nonetheless owed Wesley Greer a duty under time-honored legal principles. Experience Project, a social media website where users are encouraged to congregate and interact, is the twenty-first century equivalent of a brick-and-mortar establishment such as restaurants, bars, theaters, fairs, auditoriums, stadiums, amusement parks, and all other businesses open to the public. Under California law, a business establishment must exercise reasonable care for the safety of its invitees and is liable for injuries resulting from a breach of this duty.

VI. ARGUMENT

A. The District Court Erred in Holding That Defendant Was Not Responsible, in Whole or In Part, for the Creation or Development of the Posts Facilitating Heroin Trafficking on Its Website.

The district court incorrectly held that Section 230 precluded Plaintiff's claims, misconstruing the statute to mean that a challenge the website's recommendations functionality – which used algorithms and machine learning to identify heroin and then steer them towards heroin dealers – amounted to a challenge of "neutral tools" of the website. This misreads the Court's unambiguous authority on the scope of Section 230 immunity and fundamentally misunderstands the nature and purpose of algorithms, which despite being computer code are nonetheless suffused with their designer's intent.

Where, like here, a website is designed to intentionally perform a specific act, and this act is what gives rise to a plaintiff's claim, Section 230 immunity does not apply. Accordingly, the district court should be reversed.

i. The Scope of Section 230 Immunity Delineated By This Court

Section 230 states, in relevant part, that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C.S. § 230(c)(1). The statute defines an "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by

multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." *Id*. at § 230(f)(2).

In contrast to an interactive computer service, an "information content provider" is "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." *Id.* at § 230(f)(3). Neither "creation" nor "development" is defined in the statute.

This Court holds that Section 230 bars a plaintiff's claim against (1) a provider of an interactive computer service (2) whom a plaintiff seeks to treat as a publisher (3) of information provided by another information content provider. *Barnes v. Yahoo!, Inc*., 570 F.3d 1096, 1100-01 (9th Cir. 2009). Consistent with the definitions laid out in the statute, if the defendant website had no hand in "the creation or development" of content posted on the website, then it has immunity under Section 230, as it is an "interactive computer service." *Fair Housing Council of San Fernando Valley v. Roommates.Com*, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008) (en banc). If, on the other hand, it had a role in creating or developing the content at issue, it becomes an "information content provider," and Section 230 does not apply. *Id*.

While this Court has described the scope of Section 230's immunity in broad terms, it has also made clear that the statute does not "create a lawless no-man's-land on the internet." *Id*. at 1164.[5]

1. When a Website Materially Manipulates Third-Party Content, Creating *Additional* Content Therefrom, It "Develops" That Content and Has No Immunity Under Section 230.

The key authority in this Court that outlines the scope of Section 230 immunity is *Fair Housing Council of San Fernando Valley v. Roommates.Com*. This opinion held that a website "develops" content otherwise posted by third parties (and thus loses Section 230 immunity) when it materially manipulates that content, including by passively directing its creation or by improperly using the content, after the fact. 521 F.3d at 1168.

The defendant, Roommates.com, was a website designed to match people looking to share housing. *Id*. at 1161. In order to post or search for listings a user would have to create an account profile, in which they were required to disclose personal information including sex, family status, and sexual orientation. *Id*. Users could search for and view other profiles based on the characteristics in those profiles,

[5] *See, also, Doe v. Internet Brands, Inc.*, 824 F.3d 846, 852 (9th Cir. May 31, 2016) ("[T]he CDA does not declare a general immunity from liability deriving from third-party content.") (internal quotation marks omitted).

and based on the criteria they either posted or viewed, exchange emails with other users via the website. *Id*.

The Fair Housing Councils of the San Fernando Valley and San Diego sued the website for violating multiple housing discrimination laws, challenging the website's requirement that users include age, sex, and family status in their profiles and also challenging the website's use of those potentially discriminatory profiles in its search functionality and email notification system. *Id*. at 1162, 1165. The website claimed that its practices were shielded by Section 230, as the plaintiffs' challenges amounted to grievances over content that was posted by its users, who were the true "information content providers" in the transaction, and that the website itself was merely a passive conduit for those posts. *Id*.

This Court disagreed—while it was true that the posts were created by third parties, "the fact that users are information content providers does not preclude Roommate from *also* being an information content provider by helping 'develop' at least 'in part' the information in the profiles." *Id.* at 1165. (emphasis original). One dispositive data point was that the website was designed to guide users to disclose data about themselves that could lead to discrimination in their housing options. *Id*. This functionality, coded into the website, "materially contribute[d]" to the "alleged unlawfulness," such that the website became a co-developer of the content, and thus

became an "information content provider" that was beyond the protection of Section 230. *Id.*

Additionally, this Court held that the website "[was] not entitled to CDA immunity for the operation of its search system, which filters listings, or of its email notification system, which directs emails to subscribers according to discriminatory criteria." *Id.* at 1167.[6] The Court distinguished the defendant website's unlawful search and notification functionalities from those of "ordinary search engines," noting that the latter "do not use unlawful criteria to limit the scope of searches conducted on them, nor are they designed to achieve illegal ends." 521 F.3d at 1167. Since "Roommate's search function is…designed to steer users based on [unlawful] criteria…[it] differs materially from generic search engines such as Google, Yahoo! and MSN Live Search, in that Roommate designed its system to use allegedly unlawful criteria so as to limit the results of each search, and to force users to participate in its [unlawful] process." *Id.*

[6] This transposes identically to the facts at bar, as Plaintiff alleges that "Experience Project's recommendations functionality…—written into the website's source code—relied on data such as, but not limited to, the content of a given group, the content posted by the users within the group, and demographic data known by Experience Project about the given user, including the geographic location of the user. In point of fact, this was expressly admitted by [Experience Project CEO]: '***Immediately, you're drawn into groups that are structured around these experiences*** [that the user identifies as being relevant to himself or herself.'" Compl. at ¶ 28.

Roommates established a nuanced standard of what constitutes "development" of content under Section 230, which becomes critical for distinguishing an "interactive computer service" (who has immunity) from an "information content provider" (who does not). The Court focused on the word "development" in the definition of an "information content provider"[7] and cautioned not to "ignore[] the words 'development…in part' in the statutory passage 'creation *or development* in whole *or in part*.'" *Id.* at 1167 (quoting 47 U.S.C. § 230(f)(3)) (emphasis original). Thus, a defendant website need not author the material at issue; instead, directing its development is enough to make that website an "information content provider." *Id.*

Critically, the *Roommates* opinion explained the "definition of 'development' that is [most] suitable to the context in which we operate [is the definition] 'making usable or available.'" *Id.* at 1168. Under this standard, a website can be a developer without having created the content at issue so long as it *makes its own use* of that content in some material way. *Id*. Indisputably, under this authority, a website can face liability when it takes an active role in guiding the creation of content *or* in using that content for recommendations or email functionality (*i.e.*, steering users throughout the platform). *See*, *generally*, 521 F.3d 1157 (9th Cir. 2008).

[7] "[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). (emphasis added)

Equally instructive is *Anthony v. Yahoo! Inc.*, 421 F. Supp. 2d 1257 (N.D. Cal. 2006) a district court opinion that predates *Roommates* but that was cited approvingly by this Court in its *Roommates* analysis. 521 F.3d at 1163, n.8 (citing *Anthony*, 421 F. Supp. 2d 1257).[8] In *Anthony*, an aggrieved user of Yahoo's dating site accused the company of (1) creating fraudulent user profiles sent to lure prospective customers, and (2) sending profiles of *actual* former subscribers, whose subscriptions had lapsed, to current members of the service. *Id*. Concerning the former business practice, the district court held that Yahoo was an "information content provider" as it allegedly created the profiles at issue. *Id*. at 1262. Moreover, concerning the profiles from lapsed accounts, the court held that "[a]dmittedly, third parties created these profiles. Nevertheless, the CDA only entitles Yahoo! not to be 'the publisher or speaker' of the profiles. It does not absolve Yahoo! from liability for any accompanying misrepresentations. *Because Anthony posits that Yahoo!'s manner of presenting the profiles – not the underlying profiles themselves – constitute fraud, the CDA does not apply.*" *Id.* at 1263 (emphasis added).

Since *Roommates*, this Court has continued to hold that claims involving third-party website content do not automatically trigger Section 230 immunities.

[8] Specifically, the Court cited *Anthony* for the proposition that "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." *Roommates*, 521 F.3d at 1162-63 (citing *Anthony* v. *Yahoo! Inc.*, 421 F. Supp. 2d 1257, 1262-63 (N.D. Cal. 2006)).

Instead, where the claim focuses on conduct of the website that is separate from the third-party content, a claim is not precluded even if it indisputably relates to or is intertwined with that third-party content. For example, in *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009), a woman brought suit over a website's failure to remove nude photos of her posted by her ex-boyfriend. *Id.* at 1098. While this Court held that Section 230 precluded the plaintiff's negligence claim arising from the company's allowing the photos to be published in the first instance (*id.* at 1105-06), the Court simultaneously held that a separate, promissory estoppel claim was *not* precluded, where Yahoo had made representations to the plaintiff that it would, indeed, remove the content (*id.* at 1107-09). Although the estoppel claim unquestionably *related* to content posted by third parties, it arose from actions undertaken by Yahoo that were independent of the content's posting in the first place. *Id.*[9]

Courts in other jurisdictions follow *Roommates* and make this same, correct, distinction—recognizing that challenging a defendant's *conduct* vis-à-vis third-party content does not automatically equate to treating the website as a "publisher." *See, e.g., FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1200-01 (10th Cir. 2009) (no Section

[9] *See, also Doe v. Internet Brands, Inc.*, 824 F.3d 846, 851 (9th Cir. 2016) (failure to warn claim related to third-party posters on a website not afforded Section 230 immunity because the duty existed independently of, and had no bearing on, any specific third-party content); *Beckman v. Match.com, LLC*, 668 F. App'x 759 (9th Cir. 2016) (same).

230 immunity when defendant "solicited requests" for telephone record information, "paid researchers to find it, [and] knew that the researchers were likely to use improper methods," since its "actions were not 'neutral' with respect to generating offensive content; on the contrary, its actions were intended to generate such content.") (citing to *Fair Housing* multiple times in its analysis).[10]

The most factually apposite application of *Roommates* is a Washington state court case—*J.S. v. Vill. Voice Media Holdings, LLC*—in which three minor girls who were victims of sex trafficking sued Backpage.com, a website catering to online escort services that was used by the girls' pimps. 184 Wash. 2d 95, 359 P.3d 714 (2015) (en banc). The plaintiffs argued that Section 230 did not immunize the defendant from their claims,[11] as they alleged that the defendant's posting policies

[10] *See, also City of Chicago, Ill. v. StubHub!, Inc.*, 624 F.3d 363, 366 (7th Cir. 2010) (no Section 230 immunity for ticket-seller website accused of posting and selling tickets without remitting proper taxes, because claim relating to collection of "Chicago's amusement tax does not depend on who 'publishes' any information or is a 'speaker,'"); *Lansing v. Sw. Airlines Co.*, 980 N.E.2d 630, 639 (Ill. App. Ct. 2012) (Airline that allowed its employee to access customer information in its computer systems and harass customers could not claim Section 230 immunity because "Plaintiff's negligent supervision cause of action does not require publishing or speaking as a critical element, and holding defendant liable for its failure to supervise its employee after defendant had received notice of the employee's wrongful conduct does not treat defendant as if it were the publisher or speaker of the alleged [harassing] e-mails and texts.").

[11] The plaintiffs asserted claims for negligence, outrage, sexual exploitation of children, ratification/vicarious liability, unjust enrichment, invasion of privacy, sexual assault and battery, and civil conspiracy. *J.S. v. Vill. Voice Media Holdings, LLC*, 184 Wash. 2d 95, 98-99, 359 P.3d 714, 716 (2015).

and site functionality were specifically designed, in whole or in part, to help their pimps evade detection from law enforcement. *Id*. at 716. Citing extensively to *Roommates* throughout, the Washington Supreme Court found that the plaintiffs' allegations that Backpage "intentionally developed its website," including through developing its content guidelines and functionality, to such a degree that it evidenced collusion (and thus a co-development relationship) between the website and the pimps who trafficked the underage girls. *Id*. at 717-18. The Washington Supreme Court reversed the lower court's grant of the motion to dismiss, stating that further fact-finding was warranted "to ascertain whether in fact Backpage designed its posting rules to induce sex trafficking" and remanded the case for further proceedings. *Id* at 718.[12]

Roommates and its progeny make clear that a website need not *co-author* a third party's post to have "developed" the content pursuant to Section 230; it is

[12] Plaintiff recognizes that the First Circuit reached the opposite conclusion under similar facts and with similar arguments. *See, generally, Doe v. Backpage.com, LLC*, 817 F.3d 12 (1st Cir. 2016). This opinion is distinguishable, however, as the First Circuit was bound by different precedent employing an especially (and in Plaintiff's view, improperly) broad reading of Section 230 immunity. *Id*. at 21, n.5 ("The appellants argue that a concurring opinion in *J.S. v. Village Voice Media Holdings, L.L.C.*, 184 Wn.2d 95, 359 P.3d 714, 718-24 (Wash. 2015) (en banc) (Wiggins, J., concurring), points to a different conclusion. But our reasoning in [*Universal Commun. Sys. v. Lycos, Inc*., 478 F.3d 413 (1st Cir. 2007)] — which the J.S. concurrence failed to address — defeats this argument."). The proper analytic framework in this Court, of course, is set forth in *Roommates*, which *Doe v. Backpage.com* does not address, much less reconcile.

enough that the website manipulates the content in a unique way. This manipulation can take myriad forms, including guiding the content's generation, either through posting guidelines that signal or direct the poster,[13] content requirements for posts,[14] or even *post hoc* use of content that was generated either in whole or in part by a third party.[15]

These authorities reflect a nuanced standard set by this Court, which recognizes that websites have changed dramatically since passing of the Communications Decency Act. Most websites no longer passively "publish" a user's post to a static message board, and thus no longer serve as a mere "passive conduit" for the message. In certain circumstances, such as with social media networks like Experience Project, the relationship between the website and its users is more symbiotic, with the website taking the users' input and making its *own* derived content, then using that content for its *own* functionality and purpose.

ii. The District Court Misapplied *Roommates* by Holding That the Recommendations Functionality That Knowingly Matched Heroin Addicts to Heroin Dealers Was a "Neutral Tool," as Opposed to an Instance of Independently Developed Content.

In light of the rule established by *Roommates* and its progeny, the district court was incorrect in holding that Experience Project's manipulation of site content (and

[13] *Roommates*, 521 F.3d at 1164; *J.S.*, 359 P.3d at 717-18.
[14] *Roommates*, 521 F.3d at 1164.
[15] *Roommates*, 521 F.3d at 1164; *Anthony*, 421 F. Supp. 2d at 1263.

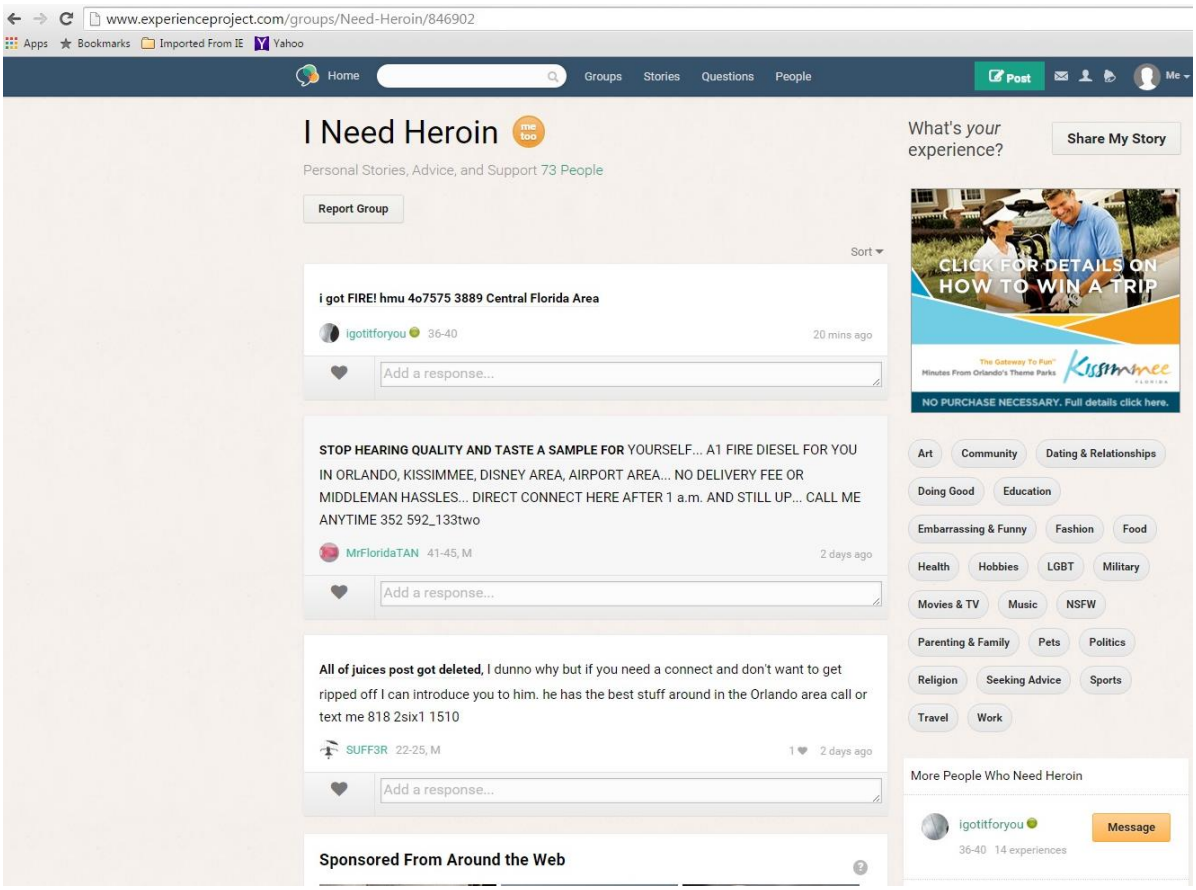
its users) did not rise to the level of "information content provider" activity. The court erroneously classified the recommendations and push notifications, which identified heroin addicts and steered them towards heroin dealers, as "content-neutral tools" and (equally erroneously) held that it was immaterial that their intent was to steer vulnerable users towards unlawful content. ER16. The court's reasoning was threefold: "[f]irst, making recommendations to website users and alerting them to posts are ordinary, neutral functions of social-network websites[;][16]…[s]econd, it is the users' voluntary inputs that create the content on Experience Project, not Ultimate Software's proprietary algorithms[17][; and]…[t]hird, the result holds even when a website collects information about users and classifies user characteristics."[18] None of these points is correct, factually or legally.

1. The Functionality Challenged by Plaintiff Involved Case-By-Case, Subjective Determinations On the Part of the Website and Its Programmers, and Cannot Be Classified as "Neutral."

First, the act of making a recommendation is, by definition, not "neutral." The district court held that "Ms. Dyroff does not plausibly allege that Ultimate Software 'promoted the use of [its neutral] tools for unlawful purposes," ER17

[16] ER16
[17] ER17
[18] ER18

(citing *Roommates.com*, 521 F.3d at 1174 n. 37) (alterations in the original), but this ignores the specific allegations in the Complaint and stretches the word "neutral" to its breaking point.[19] Instead, Defendant used its website's proprietary technology to identify Wesley Greer as a heroin addict, search through posts *it knew pertained to the sale of heroin*, and prod him—through its own, separate content—towards those posts. ER41:¶26-ER45:¶35; ER50:¶49-¶50; ER50:¶52. An example of what Wesley Greer saw is as follows:



[19] Merriam Webster defines "neutral" as "not engaged on either side" and "not decided or pronounced as to characteristics: indifferent." (https://www.merriam-webster.com/dictionary/neutral) (last visited June 12, 2018)

Fig. 1[20]

As the above demonstrates, Experience Project's recommendations functionality (shown in the bottom right corner of figure 1) was purposefully designed to engage in deliberate decision-making, and to present users with custom content, generated by Experience Project based on the decisions the website made. The act of making a recommendation is deliberative—it requires evaluating (1) the subject matter being recommended and (2) the person to whom the recommendation is being made, and making choices in light of those evaluations.

To call Experience Project's machine learning and algorithmic functionality "neutral" fundamentally misunderstands algorithms, their origin, and their purpose. Algorithms are portions of code, programmed by individuals to achieve the goals of those individuals—specifically, for the code to make decisions as those individuals' proxy. Because algorithms are the product of human endeavor, they carry all of the complexities and deliberation of human decision-making (and attendant room for error and even illegal results). This is an acknowledged problem, for instance, in the field of hiring practices and employment law. As one recent article noted, algorithms risk adopting human biases and, accordingly, effecting unlawful results:

> At their core, algorithms mimic human decision making. They are typically trained to learn from past successes, which may embed existing bias. For example, in a famous

[20] ER42:¶27

> experiment, recruiters reviewed identical resumes and selected more applicants with white-sounding names than with black-sounding ones. If the algorithm learns what a "good" hire looks like based on that kind of biased data, it will make biased hiring decisions. The result is that automatic resume screening software often evaluates job applicants based on subjective criteria, such as one's name. By latching on to the wrong features, this approach discounts the candidate's true potential.

Gideon Mann and Cathy O'Neil, "Hiring Algorithms Are Not Neutral." Harvard Business Review (Dec. 9, 2016) (available at https://hbr.org/2016/12/hiring-algorithms-are-not-neutral) (last visited June 6, 2018). The authors stress that "[a]lgorithms are, in part, our opinions embedded in code." *Id.* "In other words, *algorithms are not neutral*." *Id*. (emphasis added).

It is not speculative that biases inherent in algorithms lead to unlawfully discriminatory conduct that exists completely outside of Section 230's scope. Another article addressing this issue provides an empirical example:

> In one study, Harvard professor Latanya Sweeney looked at the Google AdSense ads that came up during searches of names associated with white babies (Geoffrey, Jill, Emma) and names associated with black babies (DeShawn, Darnell, Jermaine). She found that ads containing the word "arrest" were shown next to more than 80 percent of "black" name searches but fewer than 30 percent of "white" name searches….Sweeney worries that the ways Google's advertising technology perpetuates racial bias could undermine a black person's chances in a competition, whether it's for an award, a date, or a job.

Nanette Byrnes, "Why We Should Expect Algorithms to Be Biased," MIT Technology Review (Jun. 24, 2016) (available at https://www.technologyreview.com/s/601775/why-we-should-expect-algorithms-to-be-biased/) (last visited June 6, 2018). In the above study, Google's algorithms made deliberate, and discriminatory, choices of how to present third-party-generated content to individual users based on what it new or inferred about the users (through their search terms). Clearly, its "tools" (i.e., its algorithms) were anything but "neutral" in the presentation of this third-party-generated content.

The same holds true for Experience Project's functionalities challenged by Plaintiff in this litigation. As pled in the Complaint, Experience Project's unlawful activity took the form of, *inter alia*, (1) specifically identifying the meaning of and intent behind each and every post on its website;[21] (2) using that derived information to create *new content* that would manipulate individual users and funnel them into pockets of activity on the website, including harmful, drug-trafficking activity; (3) shielding bad actors from law enforcement requests (through both the blanket anonymity policy in its posting guidelines *and* its express antipathy towards law enforcement information requests); and (4) developing policies and procedures (and

[21] ER39:¶ 22 (citing http://www.frbsf.org/economic-research/files/wp2017-01.pdf).

engineering its software) to effectuate these goals.[22] These actions—accepted as true, taken as a whole, and interpreted with all inferences drawn in Plaintiff's favor—more than plausibly assert that Experience Project used its "tools for unlawful purposes"[23] and that those tools were not neutral. On the above facts, Plaintiff readily satisfied the pleadings requirements at the motion to dismiss stage. *Ashcroft v. Iqball*, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009) ("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.") (quoting *Twombly*, 550 U.S. at 557).

These facts also demonstrate the inapposite nature of the authority relied upon by the district court in its analysis. The court cited to a troika of cases for the proposition that website functionality is a "neutral tool." ER16-ER17 citing *Gonzalez v. Google, Inc.*, 282 F. Supp. 3d 1150 (N.D. Cal. 2017); *Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116 (N.D. Cal. 2016); *Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140 (E.D.N.Y. May 18, 2017). However, each of those cases distills to a claim

[22] *See, e.g.*, ER34¶ 6-ER35:¶8, ER38:¶19, ER39:¶22-ER40:¶23, ER41:¶26-ER48:¶42, ER50:¶52-¶53, ER55:¶70-ER56:¶71, ER56:¶73-ER57:¶74, ER61:¶94-ER62:¶96, ER63:¶105-¶106, ER65:¶115-ER66:¶117.

[23] ER17.

by a plaintiff against a website simply for allowing individuals from terrorist organizations to access the website as a normal user.[24]

Where, like here, a website's functionality is "designed to steer users based on [unlawful] criteria," its tools are not content-neutral and its behavior "differs materially from generic search engines such as Google, Yahoo! and MSN Live Search." *Roommates*, 521 F.3d at 1167. Instead, the website has "designed its system to use allegedly unlawful criteria so as to limit the results of each search, and to force users to participate in its [unlawful] process," and Section 230 does not apply. *Id.*; *Anthony*, 421 F. Supp. 2d at 1263 (Because [plaintiff] posits that Yahoo!'s *manner of presenting the profiles* – not the underlying profiles themselves – constitute fraud, the CDA does not apply.") (emphasis added). The district court was therefore in error and should be reversed.

---

[24] *See, e.g.*, *Gonzalez*, 282 F. Supp. 3d at 1165 (plaintiffs asserted "that their claims are based upon the fact that Google provides ISIS followers with access to powerful tools and equipment to publish their own content" via Google's website YouTube); *Fields*, 217 F. Supp. 3d at 1122 (plaintiffs' claims were premised on a theory of liability "based purely on Defendant's knowing provision of Twitter accounts to ISIS, not content created with those accounts."); *Cohen*, 252 F. Supp. 3d at 157 (E.D.N.Y. 2017) ("Plaintiffs argue that their claims seek to hold Facebook liable for 'provision of services' to Hamas in the form of account access 'coupled with Facebook's refusal to use available resources … to identify and shut down Hamas [] accounts.'"). Only one case, *Gonzalez*, advanced an argument that the website actually developed additional content, but this was limited to targeted advertising served on the website, generally, which is a far cry from the deliberate and specific conduct challenged in this litigation. 282 F. Supp. 3d at 1168 (N.D. Cal. 2017) (rejecting the claim by plaintiffs "that Google acts as an 'information content provider' [developing its own content] by placing targeted ads.").

2. The Website, Not Third-Party Users, Created the Harmful Content Challenged By Plaintiff.

Second, because the harmful content and conduct challenged is the recommendations functionality and push notifications, the district court was incorrect in holding that "the users' voluntary inputs…create the content on Experience Project, not Ultimate Software's proprietary algorithms." Instead, those "voluntary inputs" (like Margenat-Castro's open advertisements for heroin) merely *contribute* to Experience Project's unlawful activity and content that Plaintiff challenged in her complaint. Experience Project then took those heroin trafficking posts, determined their precise and unlawful meaning, determined the intent of the poster, and then elected to use those posts and similarly unlawful posts to entice users whom they deemed a suitable (here, vulnerable) audience. ER38:¶18-ER45:¶35.

While Section 230 might preclude a claim against a website owner for *allowing* heroin trafficking posts on their website, it does not follow that the website is shielded from knowingly steering visitors towards that content and pressuring those visitors to view and engage with the harmful posts. *Roommates*, 523 F.3d at 1165 ("[T]he fact that users are information content providers does not preclude Roommate from *also* being an information content provider by helping 'develop' at least 'in part' the information in the profiles.") (emphasis original).

In point of fact, the third-party poster has no control over the functionality that is challenged in the Complaint. Margenat-Castro had no agency in what was shown and recommended to Wesley Greer. ER46:¶36-ER48:¶42. Instead, the recommendations-based content was chosen, packaged, and presented by Experience Project. *Id.* This is precisely the type of "development…in whole or in part" contemplated by Section 230 and contextualized in this Court's holding in *Roommates*. 521 F.3d at 1168 (the "definition of 'development' that is [most] suitable to the context in which we operate [is the definition] 'making usable or available.'").[25]

[25] As with its analysis in the preceding section, the district court again relied on easily distinguishable authority. ER17-ER18, citing *Kimzey v. Yelp,* 836 F.3d 1263 (9th Cir. 2016); *Goddard v. Google*, 640 F. Supp. 2d 1193 (N.D. Cal. 2009). *Kimzey* involved a *pro se* plaintiff bringing RICO and libel claims against a website over the posting of a disparaging review from a disgruntled customer. 836 F.3d 1263 (9th Cir. 2016). The Court noted that the plaintiff's "complaint [was] far from lucid and the opening brief cryptic to the point of opacity" and that the court was forced to attempt to discern the plaintiff's relevant arguments. *Id.* at 1268. First, the court interpreted the plaintiff as claiming that Yelp, itself, wrote the disparaging review, which the court deemed were "threadbare allegations" and dismissed pursuant to *Iqbal*. *Id.* "The second, and more convoluted, [argument] is that Yelp transformed the review…into its own 'advertisement' or 'promotion' on Google and featured a unique star-rating system as the mantlepiece of its creation." *Id.* at 1269. Ultimately, it is unclear what the true allegations *were* in the case, much less how they might have any bearing on Plaintiff's underlying claims. Similarly, in *Godard*, plaintiffs brought fraud claims arising from third-party ads placed on Google's ad network. 640 F. Supp. 2d 1193 (N.D. Cal. 2009). In asserting that Google materially contributed to the third-party advertisers' fraudulent activity, the ***only*** alleged collaboration between Google and the third parties was Google's automated suggestion of the phrase "free ringtone" when an advertiser sought to place adds related to the word "ringtone." *Id*. at 1197. The plaintiff "contend[ed] that the

3. The District Court Relied on An Overly-Broad Interpretation of *Carafano*—An Opinion Abridged by *Roommates*—When It Held That Websites Cannot Co-Develop Content From Third-Party Posts.

Third, the district court erred in holding—with almost no analysis—that the fact that Experience Project "collects information about users and classifies user characteristics" was immaterial to its Section 230 analysis. ER18. Stating that Experience Project "is immune, and not an 'information content provider,' as long as users generate all content," the district court supported its reasoning with *Carafano v. Metrosplash.com, Inc*., 339 F.3d 1119, 1124 (9th Cir. 2003), an opinion that is readily distinguishable, which predates *Roommates* and which, in point of fact, required *clarification* from this Court in the *Roommates* opinion because of the "unduly broad" language in its Section 230 analysis. 521 F.3d at 1171 ("We must… clarify the reasoning undergirding our holding in *Carafano*[,] as we used language there that was unduly broad.").

In *Carafano*, the plaintiff sued a dating website after an unknown third party created a false profile containing, *inter alia*, sexually suggestive content and her phone number and address. 339 F.3d at 1121. This Court stated that the website was immune from suit under these facts—it could not "be considered an

---

suggestion of the word 'free,' when combined with Google's knowledge of the mobile content industry's unauthorized charge problems, makes the Keyword Tool neither innocuous nor neutral." *Id.* (internal quotations, citations omitted).

'information content provider' under the statute because no profile has any content until a user actively creates it." 339 F.3d 1124; *compare* ER18 ("The website is immune, and not an 'information content provider,' as long as users generate all content.") (citing *Carafano*, 339 F.3d at 1124).

In *Roommates*, this Court clarified that this was too broad a read of the statute (although the result of *Carafano* was still appropriate under a much more cabined read of Section 230's scope). This Court observed that, in *Carafano*,

> We 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."
>
> *As we explain above…even if the data are supplied by third parties, 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."*

521 F. 3d at 1171 (internal citations omitted). Ultimately,

> 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….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.

Id. at 1171-72. It is indisputable that *Carafano's* holding was cabined significantly by the above language. The district court's reliance on that opinion thus was misplaced, given the fact that it failed to take into account the clarification (and paring down) of the scope of *Carafano's* holding, as explicitly articulated in *Roommates*.

As stated above, Plaintiff's claims against the website are not "in effect, that it failed to review each user-created profile to ensure that it wasn't [unlawful]." 531 F.3d. at 1171. Instead, Plaintiff's claims are squarely grounded in *how* the "website use[d] data initially obtained from third parties," and arise from Experience Project's act of "'develop[ing]' unlawful content 'in whole or in part.'" *Id.* (alteration original). Accordingly, the district court erred in its reliance on portions of *Carafano's* holding that are inconsistent with *Roommates*.

iii. Plaintiff Plausibly Alleged Collusion Between Defendant and Its Heroin-Trafficking User Base

Separately, the district court erred in applying Section 230 despite Plaintiff's plausible allegations of Defendant's collusive activity with its criminal accountholders. Specifically, Plaintiff contended that Experience Project could not assert Section 230 immunity because it "developed" unlawful content via the policies and procedures it had established—at least in part—with knowledge and

endorsement of the illegal activity on its website, and with an intent to shield criminal users from law enforcement requests. ER18. Beyond citing to the website's strict anonymity policy, Plaintiff also cited to a March, 2016, announcement from the website that it was suspending operations, due to increased requests from law enforcement. ER18-19. In an open letter to account holders, Experience Project's CEO stated:

> From day one, **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. And you are proof that we were right! But there is no denying that the way people expect to use social media today is markedly different than it once was, and as the primary use has moved from web 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.[26]

This statement makes it indisputable that Experience Project shuttered its website, in no small part, because of law enforcement's interest in its user's activity. It is

[26] *See, also* ER47:¶41

equally indisputable that Experience Project viewed the actions of law enforcement as "aggressively attacking the foundations of internet privacy with a deluge of information requests, subpoenas, and warrants."

The district court inferred the statement in the letter unfavorably to Plaintiff, finding that "[t]his statement manifests a concern with Internet privacy that has been widespread in the technology sector and does not establish antipathy towards law enforcement especially given the statement about 'proper law enforcement requests.'" ER19. In choosing this interpretation, the district court ignored the fact that the website's CEO deemed himself arbiter of what is and is not a "proper" law enforcement request and viewed the requests directed at his website as a "deluge of information requests, subpoenas, and warrants" that "aggressively attack[ed] the foundations of internet privacy." These words plausibly demonstrate an antipathy towards law enforcement or an interest in shielding users from the prying eyes of the police, an inference the district court should have drawn in Plaintiff's favor.

On a scanter record, courts have found a level of collusion sufficient that the website's posting policies and guidelines "developed," in whole or in part, the offending third-party content, and accordingly Section 230 did not apply. As discussed above, in *J.S. v. Vill. Voice Media Holdings, LLC*, three minor girls who had been victims of human trafficking sued the website Backpage.com ("Backpage"), which their pimps utilized to traffic the girls. 184 Wash. 2d 95, 359

P.3d 714 (2015). In arguing that Section 230 did not apply to their claims against Backpage, the young women pointed to the website's posting guidelines, asserting that the site's "advertisement posting rules were 'designed to help pimps develop advertisements that can evade the unwanted attention of law enforcement, while still conveying the illegal message.'" *Id.* at 714. Critically, the pimps posted advertisements on the website "without any special guidance" or direct input from Backpage personnel, but because the website's posting guidelines prohibited posters from using certain, coded language to signal underage prostitution (yet nonetheless knew such human trafficking was occurring on its site), the plaintiffs argued that the website provided cover for the pimps to engage in their unlawful and unspeakably harmful activity. *Id.* at 716.

In an en banc opinion that relied extensively on this Court's analysis in *Roommates*, the Supreme Court of Washington held that it was enough, at the pleadings stage, for plaintiffs to allege that Backpage was aware of the human trafficking taking place on its website, and designed its posting guidelines to facilitate this bad act (by giving pimps both anonymity and plausible deniability). *Id.* at 717-18. Taking as true, *inter alia*, the plaintiffs' allegations that Backpage's posting guidelines were "a method developed by Backpage.com to allow pimps, prostitutes, and Backpage.com to evade law enforcement for illegal sex trafficking, including the trafficking of minors for sex," the court held that the website did "more

than simply maintain neutral policies prohibiting or limiting certain content," and plaintiffs had plausibly alleged development of content sufficient that Section 230 did not apply. *Id.*

This readily analogizes to the facts at bar. Like the young girls in *J.S.*, Plaintiff identified Experience Project's unlawful engagement and management of illegal activity in the form of shielding bad actors (of whom it had actual knowledge) from law enforcement review through its blanket anonymity policy and posting guidelines.[27] Going one step further than the plaintiffs in *J.S.*, Plaintiff cited to specific proof that, at least in part, the website's policies *were* created and maintained to give users cover from law enforcement, which Experience Project's CEO characterized as "aggressive[]" and "attacking the foundations of internet privacy." Plaintiff more than plausibly alleged collusion between Experience Project and its drug-trafficking users, sufficient to demonstrate at the pleadings stage that the website "contribute[d] materially to the alleged illegality of the conduct." *J.S.*, 359 P.3d at 718 (2015) (quoting *Fair Hous. Council*, 521 F.3d at 1168).

Rather than an instance of a "clever lawyer argu[ing] that *something* the website operator did encouraged the illegality," the facts at bar and the behavior at issue demonstrate an agency and intentionality on behalf of Experience Project that

[27] *See, e.g.*, ER34¶ 6-ER35:¶8, ER38:¶19, ER39:¶22-ER40:¶23, ER41:¶26-ER48:¶42, ER50:¶52-¶53, ER55:¶70-ER56:¶71, ER56:¶73-ER57:¶74, ER61:¶94-ER62:¶96, ER63:¶105-¶106, ER65:¶115-ER66:¶117.

resulted in material contribution to profoundly bad acts, thereby removing Section 230 immunity. *Roommates*, 521 F.3d at 1174-75. Because of the level of collusion and misfeasance on the part of Experience Project, Section 230 immunity does not apply and the district court should be reversed.

iv. The District Court Erred in Holding That No Duty Was Owed to Wesley Greer

In dismissing Plaintiff's failure to warn claim,[28] the district court erred in holding that Experience Project did not owe a duty of care to Wesley Greer, both due to its own misfeasance and due to the general duty owed by a social media website to its users.

1. Defendant's Misfeasance Created a Duty Owed to Wesley Greer.

Under California law, in determining whether a defendant owes a duty to a plaintiff in a particular case, courts distinguish between misfeasance and nonfeasance. *See, e.g., Seo v. All-Makes Overhead Doors*, 97 Cal. App. 4th 1193, 1202, 119 Cal. Rptr. 2d 160 (2002). "Misfeasance exists when the defendant is responsible for making the plaintiff's position worse, i.e., defendant has created a

[28] Specifically, Plaintiff contended that Experience Project had actual knowledge of the fact that Margenat-Castro was purporting to sell heroin on the website, when in fact it was pure fentanyl, and that the website's failure to warn Wesley Greer of this fact led to his overdose and homicideER63:¶102-ER64:¶111. This Court holds that Section 230 does not apply to failure to warn claims. *Doe v. Internet Brands, Inc.*, 824 F.3d 846 (9th Cir. May 31, 2016).

risk. Conversely, nonfeasance is found when the defendant has failed to aid plaintiff through beneficial intervention." *Weirum v. RKO Gen., Inc.*, 15 Cal. 3d 40, 49, 123 Cal. Rptr. 468, 539 P.2d 36 (1975). In cases of misfeasance, the question of duty is governed by the standards of ordinary care, i.e. "a person ordinarily is obligated to exercise due care in his or her own actions so as not to create an unreasonable risk of injury to others, and this legal duty generally is owed to the class of persons who it is reasonably foreseeable may be injured as the result of the actor's conduct." *Lugtu v. California Highway Patrol*, 26 Cal. 4th 703, 716, 110 Cal. Rptr. 2d 528, 28 P.3d 249 (2001). *See also* Cal. Civ. Code § 1714 ("Everyone is responsible, not only for the result of his or her willful acts, but also for an injury occasioned to another by his or her want of ordinary care or skill in the management of his or her property or person, except so far as the latter has, willfully or by want of ordinary care, brought the injury upon himself or herself.").

Stating that Plaintiff simply "contend[ed] that [Experience Project] created a risk of harm through its website functionalities and thus owed her son an ordinary duty of care," the district court held that Experience Project's "use of the neutral tools and functionalities on its website" did not rise to misfeasance. ER26. However, as stated in Sections VI.A.ii.1 and VI.A.ii.2, this mischaracterizes not only the intentionality and effect of the challenged functionalities, but also Experience Project's own commitment to allowing illegal activity on its website. Where an

entity knowingly identifies heroin addicts and knowingly steers them towards heroin dealers, and where that same website intentionally seeks to hide that unlawful behavior from law enforcement, it has created a risk through its own misfeasance. *Weirum*,15 Cal. 3d at 49. Because the functionalities were *not* neutral, and because Experience Project purposely sought to create an environment that shielded bad actors, it owed a duty of care to Wesley Greer for the risk it helped create, and the district court erred in holding otherwise.

2. California Law Recognizes a Special Relationship in Circumstances Analogous to Social Media Websites.

As stated in Plaintiff's Complaint, a social network like Experience Project, with its business model of building and cultivating "communities" and "groups," is the twenty-first century equivalent of a brick and mortar business establishment. Just like restaurants, bars, theaters, fairs, auditoriums, stadiums, amusement parks, and all other businesses open to the public, Defendant enticed members of the public to congregate on Experience Project website in furtherance of Defendant's business interest and in a manner entirely consonant with traditional concepts of public gathering. Compl. at ¶¶ 88-91.

In defining the scope of the duty owed by a business establishment to its invitees, the California Supreme Court stated that a "proprietor is…required to exercise reasonable care for the[] safety [of invitees] and is liable for injuries resulting from a breach of this duty." *Taylor v. Centennial Bowl, Inc.*, 65 Cal. 2d

114, 121, 52 Cal. Rptr. 561, 565, 416 P.2d 793, 797 (1966). The duty includes "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." *Id.*

Plaintiff's position that a website is akin to a physical business finds support in the law. In *Ebay, Inc. v. Bidder's Edge, Inc*., 100 F. Supp. 2d 1058 (N.D. Cal. 2000), eBay sought a preliminary injunction to prevent another website from sending "web crawlers" (programs that scan a website's HTML code) to eBay's website to obtain information about the various auctions that were occurring at any given time. One of eBay's causes of action was trespass, and it illustrated this claim by describing the defendant's behavior "as equivalent to sending in an army of 100,000 robots a day to check the prices in a competitor's store." *Id*. at 1065. The court noted that any distinction between eBay (a virtual store) and a brick and mortar store would be "formalistic" and stated, in an explanatory footnote, that the modern trend was moving from physical to online business. *Id*. at 1065, n.11. The court concluded that the defendant's behavior not only *was* a trespass, it was "*more akin to the traditional notion of a trespass to real property, than the traditional notion of a trespass to chattels*." *Id.* at 1067 (emphasis added). A portion of the court's analysis rested on the fact that the information requests sent from defendant's computers to eBay's servers were sufficiently "tangible" to equate to defendant's physical

presence (and thus interference) of eBay's property. *Id.* at 1069 ("It appears likely that the electronic signals sent by [the defendant] to retrieve information from eBay's computer system are . . . sufficiently tangible to support a trespass cause of action."); *see also Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1566-67, 54 Cal. Rptr. 2d 468, 473 (1996) (same); *Compuserve Inc. v. Cyber Promotions*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (same); *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 438 (2d Cir. 2004) ("Verio likely committed a trespass by using a search robot to access Register.com's computer systems without authorization to do so.") (citing *eBay*, 100 F.Supp.2d at 1071, for the brunt of its analysis).

The same applies when an individual visits a website: when Wesley Greer visited the Experience Project website, HTTP requests were sent by his browser to Experience Project's server and that quantum of physical presence and connection was just as material in that moment as it was in *eBay* and the other, above cases. The district court conceded that the reasoning in *eBay* was sound and that a physical connection joined the parties—"[*eBay's*] result makes sense: there was a threatened physical incursion onto eBay's website" (ER25:n.56)—but failed to explain why, considering that parties physically "visit" websites when they load their content from their servers, it does not follow that websites may (and should) be treated as physical businesses.

Nor was the district court correct in its analysis that "[r]isk can be more apparent in the real world than in the virtual social-network world." ER25. The record is replete with allegations that Experience Project claimed to know *the meaning and intention* behind *every* post of *every* user. ER38:¶18-ER45:¶35. If anything, the district court's logic militates *in favor* of Plaintiff's position, since in the brick-and-mortar world, a business establishment cannot monitor every single invitee or encounter on its premises (yet has a duty to exercise ordinary care in doing just that). In the virtual world, the opposite is true. A company like Experience Project specifically designs its website to be a panopticon that mines, records, analyzes and stores every interaction taking place on its premises. *Id*. Under the district court's logic, it would be unfair to *brick-and-mortar establishments* to hold them to the same monitoring standards as social media websites. Not the other way around.

Although incorrectly applied by the district court, the above case law, analogizing websites to "brick and mortar" businesses for purposes of tort analysis in the trespass context, resolves the doubts expressed by other courts tasked with analyzing the relationship between websites and visitors, and acknowledging that there is a lack of California law to resolve this "difficult question." *Doe v. Internet Brands,* No. 2:12-cv-3626-JFW (PJW), ECF. No. 51at *5 (C.D. Cal. November 14, 2016). Since a special relationship existed between Experience Project (a business

proprietor) and its accountholder Wesley Greer (an invitee),[29] a duty was owed. *Id.* ("'Special relationships' that courts have found to trigger a duty to protect another from foreseeable injury caused by a third party include…those between…business proprietors…and their tenants, patrons, or invitees."); *accord Beckman v. Match.com*, No. 2:13-cv-00097-JCM-NJK, ECF No. 43, at *4 (Dist. Nev. March 10, 2017). The district court erred in reaching the opposite conclusion.

VII. CONCLUSION

Section 230 was *not* introduced to transform the internet into a lawless vacuum in which the vulnerable are preyed upon and left with no recourse, yet this is what the district court's reading of Section 230 immunity achieves. This Court made clear that such a result must be avoided:

> The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant—perhaps the preeminent—means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.

[29] *See, Ebay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000); *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1566-67, 54 Cal. Rptr. 2d 468, 473 (1996); *Compuserve Inc. v. Cyber Promotions*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997); *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 438 (2d Cir. 2004)

Roommates, 521 F.3d at 1164 n.15. Plaintiff is both cognizant of and sympathetic to Section 230's goal to protect "Good Samaritan" websites from any liability they might be exposed to in attempting to curb abuse across their service. But Plaintiff is not trying to impose liability on good Samaritans. She is seeking to hold Defendant liable for its own bad acts.

For the reasons stated herein, the district court's decision should be reversed.

Dated: June 13, 2018

Respectfully submitted,

/s/ David Slade

David Slade
Carney Bates & Pulliam, PLLC
519 W. 7th St.
Little Rock, AR 72201
Phone: 501-312-8500
Fax: 501-312-8505

Sin-Ting Mary Liu
Aylstock, Witkin, Kreis, & Overholtz, PLLC
875-A Island Drive #144
Alameda, CA 94502
mliu@awkolaw.com
Phone: 510-698-9566
Fax: 760-304-8933

Attorneys for Plaintiff-Appellant, Kristanalea Dyroff

CERTIFICATE OF COMPLIANCE
Pursuant to 9th Circuit Rule 32-1 for Case Number 18-15175

I certify that: This brief complies with the length limits permitted by Ninth Circuit Rule 32-1. The brief is 12,003 words, excluding the portions exempted by Def. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

Executed on June 13, 2018.

/s/ David Slade
David Slade

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on June 13, 2018.

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

Dated: June 13, 2018

/s/ David Slade
David Slade