

RECEIVED

JAN 25 2019

CLERK OF SUPREME COURT
OF WISCONSIN

Supreme Court of Wisconsin

YASMEEN DANIEL, Individually, and as
Special Administrator of the Estate of Zina Daniel Haughton,
Plaintiff-Appellant,

TRAVELERS INDEMNITY COMPANY OF CONNECTICUT,
as Subrogee for Jalisco's LLC,
Intervening Plaintiff,

v.

ARMSLIST, LLC, an Oklahoma Limited Liability Company,
BRIAN MANCINI and JONATHAN GIBBON,
Defendants-Respondents-Petitioners,

BROC ELMORE, ABC INSURANCE CO., the fictitious name for an unknown insurance
company, DEF INSURANCE CO., the fictitious name for an unknown insurance company, and
ESTATE OF RADCLIFFE HAUGHTON, by his Special Administrator, Jennifer Valenti,
Defendants,

PROGRESSIVE UNIVERSAL INSURANCE COMPANY,
Intervening Defendant.

Appeal No. 2017AP344
Milwaukee County Circuit Court Case No. 2015CV8710

BRIEF OF AMICUS CURIAE COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION

Counsel for Amicus Curiae CCIA

PERKINS COIE LLP
Andrew T. Dufresne
State Bar No. 1081409
33 East Main Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 663-7492
Facsimile: (608) 663-7499
ADufresne@perkinscoie.com

Of Counsel

WILSON SONSINI GOODRICH & ROSATI
PROFESSIONAL CORPORATION
Brian M. Willen
Jason B. Mollick
1301 Avenue of the Americas, 40th Floor
New York, New York 10019
Telephone: (212) 999-5800
Facsimile: (212) 999-5899
bwillen@wsgr.com
jmollick@wsgr.com

TABLE OF CONTENTS

INTRODUCTION 1

I. Congress Determined That Traditional Standards of Publisher
and Distributor Liability Should Not Apply on the Internet.....2

II. Section 230 Immunizes Online Service Providers from Claims
Arising from Content Posted by Third Parties.....3

III. The Court of Appeals Misapplied Section 230.....5

 A. The Decision Below Misinterprets the CDA as a
 Narrow Immunity That Cannot Protect the “Design
 and Operation” of a Website.....5

 B. The Court of Appeals Should Have Applied the
 “Material Contribution Test” to Determine Whether
 Defendants are “Information Content Providers”10

CONCLUSION.....15

TABLE OF AUTHORITIES

CASES

<i>Barnes v. Yahoo!, Inc.</i> , 570 F.3d 1096 (9th Cir. 2009)	4, 13, 14
<i>Barrett v. Rosenthal</i> , 40 Cal. 4th 33 (2006)	4
<i>Cohen v. Facebook, Inc.</i> , 252 F. Supp. 3d 140 (E.D.N.Y. 2017)	6, 7
<i>Courtney v. Vereb</i> , No. 12-655, 2012 U.S. Dist. LEXIS 87286 (E.D. La. June 21, 2012).....	4
<i>Doe v. Backpage.com, LLC</i> , 817 F.3d 12 (1st Cir. 2016).....	7
<i>Doe v. MySpace, Inc.</i> , 528 F.3d 413 (5th Cir. 2008)	6, 7, 9
<i>Dyoff v. Ultimate Software Grp., Inc.</i> , No. 17-cv-05359-LB, 2017 U.S. Dist. LEXIS 194524 (N.D. Cal. Nov. 26, 2017)	8, 12
<i>Fair Hous. Council v. Roommates.com, LLC</i> , 521 F.3d 1157 (9th Cir. 2008)	10, 11, 13
<i>Fields v. Twitter, Inc.</i> , 217 F. Supp. 3d 1116 (N.D. Cal. 2016).....	8
<i>FTC v. Accusearch, Inc.</i> , 570 F.3d 1187 (10th Cir. 2009)	6, 10, 11, 12
<i>Gonzalez v. Google, Inc.</i> , 282 F. Supp. 3d 1150 (N.D. Cal. 2017).....	6, 8

<i>Hassell v. Bird</i> , 5 Cal. 5th 522 (2018)	4
<i>Herrick v. Grindr, LLC</i> , 306 F. Supp. 3d (S.D.N.Y. Jan. 25, 2018)	8
<i>J.S. v. Vill. Voice Media Holdings, LLC</i> , 359 P.3d 714 (Wash. 2015)	12, 13
<i>Jones v. Dirty World Entm't Recordings LLC</i> , 755 F.3d 398 (6th Cir. 2014)	2, 3, 4, 11
<i>Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.</i> , 591 F.3d 250 (4th Cir. 2009)	7
<i>Shiamili v. Real Estate Grp. of N.Y., Inc.</i> , 17 N.Y.3d 281 (2011)	3
<i>Universal Commc'ns. Sys. v. Lycos, Inc.</i> , 478 F.3d 413 (1st Cir. 2007)	7, 8
<i>Zeran v. Am. Online, Inc.</i> , 129 F.3d 327 (4th Cir. 1997)	2, 3, 4

STATUTES

47 U.S.C. § 230	<i>passim</i>
-----------------------	---------------

INTRODUCTION

For over 20 years, online service providers have relied upon an established body of law interpreting Section 230 of the Communications Decency Act (“Section 230” or the “CDA”), which delineates the extent to which they can or cannot be responsible for the activities of third-party users. The Court of Appeals broke with decades of case law interpreting the CDA as a broad immunity for the “traditional editorial functions” of online service providers, and instead adopted an idiosyncratic “plain language interpretation” that Section 230 does not protect the “design and operation of website features.” The untenable result is that the CDA now means something different in Wisconsin than it does everywhere else.

The Computer and Communications Industry Association (“CCIA”) is comprised of companies in the high-technology products and services sectors—companies that provide a broad range of online services to billions of people around the world. Although CCIA takes no position on whether Defendants in this case are protected by Section 230, it is imperative that this Court reject the Court of Appeals’ unprecedented interpretation—and thereby ensure national uniformity in the application—of this vital federal statute.

ARGUMENT

I. CONGRESS DETERMINED THAT TRADITIONAL STANDARDS OF PUBLISHER AND DISTRIBUTOR LIABILITY SHOULD NOT APPLY ON THE INTERNET

Section 230 “immunizes providers of interactive computer services against liability arising from content created by third parties.” *Jones v. Dirty World Entm’t Recordings LLC*, 755 F.3d 398, 406 (6th Cir. 2014). Section 230(c)(1) mandates 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). Subject to limited exceptions, “[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.” *Id.* § 230(e)(3).

“Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.” *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997). Congress understood that if online providers were subject to traditional publisher or distributor liability whenever third-party information is posted to, or accessible through, their services, they would be forced to investigate each and every notice of potentially unlawful

activity. “Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context.” *Id.* at 333. As the Sixth Circuit has explained, barring publisher liability against online services “serves three main purposes. First, it maintains the robust nature of Internet communication and, accordingly, keeps government interference in the medium to a minimum.... Second, the immunity provided by § 230 protects against the ‘heckler’s veto’ that would chill free speech.... Third, § 230 encourages interactive computer service providers to self-regulate.” *Jones*, 755 F.3d at 407-08 (citations omitted).

II. SECTION 230 IMMUNIZES ONLINE SERVICE PROVIDERS FROM CLAIMS ARISING FROM CONTENT POSTED BY THIRD PARTIES

“Both state and federal courts around the country have generally interpreted Section 230 immunity broadly, so as to effectuate Congress’s policy choice ... not to deter harmful online speech through the ... route of imposing tort liability on companies that serve as intermediaries for other parties’ potentially injurious messages[.]” *Shiamili v. Real Estate Grp. of N.Y., Inc.*, 17 N.Y.3d 281, 288 (2011) (citations omitted). Countless courts have interpreted Section 230 to bar “any cause of action that would make service providers liable for information originating with a third-party user

of the service.” *Jones*, 755 F.3d at 406-07 (emphasis added; citations omitted; collecting cases):

[M]any causes of action might be premised on the publication or speaking of what one might call “information content.” A provider of information services might get sued for violating anti-discrimination laws, for fraud, negligent misrepresentation, and ordinary negligence, for false light, or even for negligent publication of advertisements that cause harm to third parties. Thus, what matters is not the name of the cause of action—defamation versus negligence versus intentional infliction of emotional distress—what matters is whether the cause of action inherently requires the court to treat the defendant as the “publisher or speaker” of content provided by another.

Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1101-02 (9th Cir. 2009) (citations omitted).

Under this standard, virtually every court to have interpreted Section 230 has held that it bars “lawsuits seeking to hold a service provider liable for its exercise of a publisher’s traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content” that they did not themselves create. *Zeran*, 129 F.3d at 330; *accord, e.g., Jones*, 755 F.3d at 407 (immunizing a service provider’s exercise of “traditional editorial functions” goes to the “core” of Section 230).¹

¹ Far from being “discredited,” as Plaintiff claims without any support (Pl. Br. at 39), *Zeran* is widely considered to be the “leading case on section 230 immunity.” *Hassell v. Bird*, 5 Cal. 5th 522, 535 (2018) (quoting *Barrett v. Rosenthal*, 40 Cal. 4th 33, 41, 46 (2006) (“The *Zeran* court’s views have been broadly accepted, in both federal and state courts.”)); *accord, e.g., Courtney v. Vereb*, No. 12-655, 2012 U.S. Dist. LEXIS 87286, at *8 (E.D. La. June 21, 2012) (*Zeran* is “[o]ne of the most important and oft-cited cases on CDA immunity”).

III. THE COURT OF APPEALS MISAPPLIED SECTION 230

A. The Decision Below Misinterprets the CDA as a Narrow Immunity That Cannot Protect the “Design and Operation” of a Website

The Court of Appeals in this case broke from this established consensus. The Court instead engaged in an idiosyncratic—and unprecedented—interpretation of Section 230, finding only a “narrow scope of immunity” applied directly to user communications themselves. Op. ¶¶ 27, 34, 42, 47 & n.5. It refused to apply Section 230 because Plaintiff does not (in the Court’s view) “seek to hold Armslist liable for publishing another’s information content. Instead, the claims seek to hold Armslist liable for its own alleged actions in *designing and operating its website* in ways that caused injuries to Daniel,” i.e., by “facilitat[ing] illegal firearms purchases” between third parties communicating on the site. *Id.* ¶¶ 3, 19, 51-52 (emphasis added).

That approach has been rejected by every court to have considered it. As court after court has explained, “Section 230(c)(1) is implicated not only by claims that *explicitly* point to third party content but also by claims which, though artfully pleaded to avoid direct reference, *implicitly* require recourse to that content to establish liability or implicate a defendant’s role,

broadly defined, in publishing or excluding third party communications.”

Cohen v. Facebook, Inc., 252 F. Supp. 3d 140, 155-58 (E.D.N.Y. 2017) (emphasis added) (barring claims that Facebook “contributed to” unlawful conduct by allowing persons to create accounts and post offensive content on its service, because “Facebook’s role in publishing [third-party] content is thus an essential causal element of the claims”); *see also, e.g., FTC v. Accusearch Inc.*, 570 F.3d 1187, 1197 (10th Cir. 2009) (rejecting argument that CDA did not cover a website’s “conduct” in facilitating the posting of confidential telephone information, “rather than for the content of the information,” because ultimately the website “would not have violated the FTCA had it not ‘published’ the confidential telephone information”);

Gonzalez v. Google, Inc., 282 F. Supp. 3d 1150, 1164-65 (N.D. Cal. 2017) (rejecting argument that CDA does not bar claims alleging “provision of material support” to persons inciting violence online, because “[t]his argument essentially tries to divorce [a third party’s] offensive content from the ability to post such content”); *Doe v. MySpace, Inc.*, 528 F.3d 413, 420 (5th Cir. 2008) (noting “fallacy” in plaintiffs’ argument that “they only seek to hold MySpace liable for its failure to implement measures that would have prevented” minors from communicating on the site, because “[t]heir

allegations are merely another way of claiming that MySpace was liable for publishing the communications and they speak to MySpace's role as a publisher of online third-party-generated content").

Accordingly, it is well settled that "decisions as to the 'structure and operation' of a website ... fall within Section 230(c)(1)'s protection[.]" *Cohen*, 252 F. Supp. 3d at 156-57. Courts uniformly hold that the CDA "address[es] the structure and operation of [a defendant's] website, that is, [defendant's] decisions about how to treat postings.... Features such as these, which reflect choices about what content can appear on the website and in what form, are editorial choices that fall within the purview of traditional publisher functions." *Doe v. Backpage.com, LLC*, 817 F.3d 12, 16-17, 21 (1st Cir. 2016) (barring claim that defendant structured website to facilitate unlawful user transactions); *see also, e.g., Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 256-58 (4th Cir. 2009) (defendant immunized from claim that "structure and design of its website" facilitated tortious content); *Universal Comm'n Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 418-22 (1st Cir. 2007) ("Lycos's decision not to reduce misinformation by changing its web site policies was as much an editorial decision with respect to that misinformation as a decision not to delete a

particular posting.”); *Dyroff v. Ultimate Software Grp., Inc.*, No. 17-cv-05359-LB, 2017 U.S. Dist. LEXIS 194524, at *18-19 (N.D. Cal. Nov. 26, 2017) (rejecting plaintiff’s attempt to “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”); *Herrick v. Grindr, LLC*, 306 F. Supp. 3d 579, 588-93 (S.D.N.Y. 2018) (“Herrick’s claim that Grindr is liable because it failed to incorporate adequate protections against impersonating or fake accounts is just another way of asserting that Grindr is liable because it fails to police and remove impersonating content.... [T]hese features (or the lack of additional capabilities) are ... exactly the sort of ‘editorial choices’ that are a function of being a publisher.”) (citations omitted); *Gonzalez*, 282 F. Supp. 3d at 1166 (barring claim that “functionality” of YouTube’s service “enhance[d] [third-party’s] ability to conduct [unlawful] operations”); *Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116, 1124 (N.D. Cal. 2016) (“Twitter’s decisions to structure and operate itself as a platform ... reflect choices about what [third-party] content can appear on [Twitter] and in what form. Where such choices form the basis of a plaintiff’s claim, section 230(c)(1) applies.”) (citations omitted).

Here, however, the Court of Appeals tried to divorce the “design and operation” of Defendants’ website from claims based on third-party content posted on that site, and Plaintiffs echo this mistake in their arguments to this Court. Their claims only underscore the logical “fallacy” of that distinction. *MySpace*, 528 F.3d at 420. Plaintiffs’ theory is that an online platform “is liable for designing and operating its website in a way that encouraged prohibited sales[.]” Op. ¶ 35. But, of course, those sales were only “encouraged” because the website’s “features” enabled users to *connect and communicate with one another on the site*. *Id.* ¶¶ 13, 19. Thus, Plaintiffs are ultimately seeking to hold a website liable for its role in facilitating third-party communications. *Id.* Without those communications, there could be no claim of liability.

At bottom, then, Plaintiffs’ arguments are premised on the notion that a website can be held liable for the actions of its users where it, allegedly, did not do enough to stop those users from posting advertisements that might result in unlawful sales. That theory does exactly what Section 230 forbids: premise liability on the choices an online service provider makes about what “information provided by another information content provider” should or should not appear on its site. Imposing liability

on such core publisher activity impermissibly treats the service provider as the “publisher or speaker” of material supplied by its users. Under the correct interpretation of the statute, Section 230 applies to any claims that “can be boiled down to the failure of an interactive computer service to edit or block user-generated content that it believes was tendered for posting online, as that is the very activity Congress sought to immunize by passing the section.” *Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157, 1172 n.32 (9th Cir. 2008).

B. The Court of Appeals Should Have Applied the “Material Contribution Test” to Determine Whether Defendants are “Information Content Providers”

No one suggests that Section 230 immunity is unlimited. “[A]n interactive computer service that is also an ‘information content provider’ of certain content is not immune from liability arising from publication of that content.” *Accusearch*, 570 F.3d at 1197. Accordingly, instead of discarding Section 230 outright based on a false distinction between a website’s “content” and “design,” the Court of Appeals should have followed established law to determine whether Defendants are themselves “information content provider[s]” and therefore “responsible, in whole or in part,” for creating or developing illegality. 47 U.S.C. § 230(f)(3).

Under the “material contribution” test, “a website helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct.” *Roommates.com*, 521 F.3d at 1167-68. Importantly, however, a “material contribution to the alleged illegality of the content does not mean merely taking action that is necessary to the display of allegedly illegal content. Rather, it means being responsible for what makes the displayed content allegedly unlawful.” *Jones*, 755 F.3d at 410. The service must have contributed to the illegality *intentionally*, such as in *Roommates.com* where the defendant (which had been sued for soliciting discriminatory information in violation of the Fair Housing Act) deliberately “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 discriminatory process.” 521 F.3d at 1167. By contrast, merely “providing *neutral tools* to carry out what may be unlawful or illicit searches does not amount to ‘development’ for purposes of the immunity exception.” *Id.* at 1169 (emphasis added); *see also Jones*, 755 F.3d at 416.

As another example, in *FTC v. Accusearch*, the Tenth Circuit held that “a service provider is ‘responsible’ for the development of offensive

content only if it in some way specifically encourages development of what is offensive about the content.” 570 F.3d at 1199. The court held that the defendant, which had actively solicited and paid for confidential telephone records to be posted and sold on its website, was “not ‘neutral’ with respect to generating offensive content; on the contrary, its actions were *intended* to generate such content.” *Id.* at 1201 (emphasis added).

Courts around the country have applied this framework in a variety of contexts, including in cases like this one, where defendants allegedly “knew or should have known” that website “functionalities” might facilitate unlawful transactions between users. *E.g., Dyroff*, 2017 U.S. Dist. LEXIS 194524, at *19-29 (“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*. 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’ information, even in part.”) (emphases added; citations omitted).

The “material contribution” test was also applied in a case invoked by Plaintiff, *J.S. v. Village Voice Media Holdings, LLC*, where it was

alleged that defendant intentionally designed its website to facilitate unlawful transactions between users. 359 P.3d 714, 717-18 (Wash. 2015) (“It is important to ascertain whether in fact Backpage designed its posting rules to induce sex trafficking to determine whether Backpage is subject to suit under the CDA because ‘a website helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct.’”) (quoting *Roommates.com*).

While CCIA takes no position on the outcome of the “material contribution” test when properly applied in this case, the Court of Appeals departed from established law by ignoring that test and jettisoning any possible Section 230 protection, simply because (in its view) Plaintiff seeks to hold Defendants responsible for the “design and operation” of their website. The Court itself admitted that this idiosyncratic view conflicts with authority throughout the country. Op. ¶¶ 34-36, 48-51.

Indeed, even the cases the Court of Appeals considered “persuasive” do not support its analysis. *Id.* ¶¶ 45-46. The Court relied heavily upon a *concurring* opinion in *J.S.*, but ignored the *majority’s* use of the “material contribution” test. 359 P.3d at 717-18. The Court also invoked *Barnes*,

which found that a defendant's contractual promise to remove content may waive the CDA safe harbor, but otherwise endorsed a broad immunity covering "a publisher's traditional editorial functions," such as "reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content." 570 F.3d at 1101-02.


Plaintiff, too, cites cases that supposedly embrace a "narrow construction of the CDA." Pl.'s Br. at 31-34. None of them actually do. The vast majority featured allegations that defendants themselves created or actively solicited unlawful content (*Bay Parc Plaza Apartments, Congoo, Opperman, Perkins, Moving & Storage, Stevo Design, LeanSpa, CYBERsitter, Fraley, Alvi Armani Medical, Anthony, Hy Cite, MCW, Huon, Backpage II*). Others concerned ordinances or private suits that did not involve third-party content (*Doe v. Internet Brands, StubHub!, Airbnb, Homeaway.com, Sigler, Maynard, McDonald*). None of those cases found that the "design and operation" of a website falls outside the CDA, irrespective of whether it "contributes materially" to illegality, or merely offers "neutral tools" to third parties. On that, the Court of Appeals stands entirely alone. And its approach is neither compelled by the text of the statute nor compatible with the enormous body of robust Section 230 case

law. This Court should bring Wisconsin in line with this long-established consensus.

CONCLUSION

The decision below broke with two decades of established case law and threatens to substantially erode the protections that Section 230 affords to all service providers—not just Defendants. Unless reversed, plaintiffs with creative lawyers will come to Wisconsin to exploit this loophole and pursue claims that have consistently been understood as prohibited in every other state.

Dated: January 25, 2019

By: 

Andrew T. Dufresne
State Bar No. 1081409
PERKINS COIE LLP
33 East Main Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 663-7492
Facsimile: (608) 663-7499
ADufresne@perkinscoie.com

Counsel for Amicus Curiae CCIA

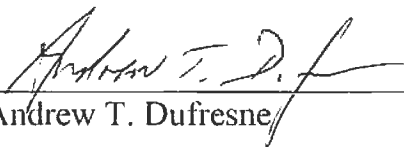
Brian M. Willen
Jason B. Mollick
WILSON SONSINI GOODRICH &
ROSATI, PC
1301 Avenue of the Americas,
40th Floor
New York, New York 10019
Telephone: (212) 999-5800
Facsimile: (212) 999-5899
bwillen@wsgr.com
jmollick@wsgr.com

Of Counsel

FORM AND LENGTH CERTIFICATION

I hereby certify that this brief conforms to the rules contained in Wis. Stat. § 809.19(8)(b)-(d) for a non-party brief produced with a proportional serif font. The length of this brief is 2,997 words.

Dated: January 25, 2019



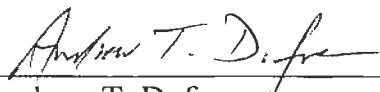
Andrew T. Dufresne

Counsel for Amicus Curiae CCIA

CERTIFICATION REGARDING ELECTRONIC BRIEF

I hereby certify that I have submitted an electronic copy of this brief which complies with the requirements of Wis. Stat. § 809.19(12). I further certify that the text of the electronic copy of this brief is identical to the text of the paper copy of the brief filed as of this date.

Dated: January 25, 2019



Andrew T. Dufresne

Counsel for Amicus Curiae CCIA

CERTIFICATE OF SERVICE

I certify that on this 25th day of January 2019, I caused a copy of this brief to be served upon each of the following parties via e-mail or U.S.

Mail:

QUARLES & BRADY LLP
Joshua D. Maggard
Eric J. Van Schyndle
411 East Wisconsin Avenue
Suite 2400
Milwaukee, WI 53202

joshua.maggard@quarles.com
eric.vanschyndle@quarles.com

MANATT, PHELPS &
PHILLIPS, LLP
Jacqueline C. Wolff
Samantha J. Katze
7 Times Square
New York, NY 10036

jwolff@manatt.com
skatze@manatt.com

CANNON & DUNPHY
Patrick O. Dunphy
Brett A. Eckstein
594 North Barker Road
P.O. Box 1750
Brookfield, WI 53008

pdunphy@c-dlaw.com
beckstein@c-dlaw.com

REED SMITH LLP
Brian A. Sutherland
101 Second Street
Suite 1800
San Francisco, CA 94105

bsutherland@reedsmith.com

BRADY CENTER TO PREVENT
GUN VIOLENCE LEGAL
ACTION PROJECT
Jonathan E. Lowy
Alla Lefkowitz
840 First Street, NE
Suite 400
Washington, D.C. 20002

CHAPIN & ASSOCIATES
John A. Griner
13935 Bishops Drive
Suite 250
Brookfield, WI 53005

FUCHS & BOYLE SC
John F. Fuchs
13500 Watertown Plank Road
Suite 100
Elm Grove, WI 53122

DEVINE HAHN SC
Thomas M. Devine
Anthony P. Hahn
840 Lake Avenue
Suite 300
Racine, WI 53403

tdevine@hhb.com
ahahn@hhb.com

KRAVIT, HOVEL & KRAWCZYK SC
Brian T. Fahl
825 N. Jefferson Street, 5th Floor
Milwaukee, WI 53202

btf@kravitlaw.com

MENN LAW FIRM LTD.
Crystal Abbey
2501 E. Enterprise Avenue
P.O. Box 785
Appleton, WI 54912

Crystal-Abbey@mennlaw.com

SKADDEN, ARPS, SLATE,
MEAGHER & FLOM LLP
Anthony J. Dreyer
Elizabeth A. Hellman
Naomi S. Solomon
4 Times Square
New York, NY 10036

anthony.dreyer@skadden.com

STAFFORD ROSENBAUM LLP
Gregory Matthew Jacobs
Jeffrey A. Mandell
222 W. Washington Avenue
Suite 900
Madison, WI 53701

gjacobs@staffordlaw.com
jmandell@staffordlaw.com

PETERSON, BERK & CROSS S.C.
John C. Peterson
Emily I Lonergran
200 E. College Avenue
P.O. Box 2700
Appleton, WI 54912

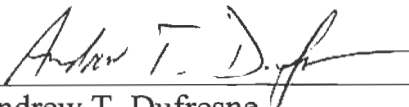
KRAMER LEVIN
Karen S. Kennedy
Michael J. Dell
1177 Avenue of the Americas
New York, NY 10036

kkennedy@kramerlevin.com
mdell@kramerlevin.com

GIMBEL, REILLY, GUERIN &
BROWN LLP
Kathryn A. Keppel
Steven C. McGaver
Catherine R. Gellis
330 E. Kilbourne Avenue
Suite 1170
Milwaukee, WI 53202

kkeppel@grgblaw.com
smcgaver@grgblaw.com

Dated: January 25, 2019



Andrew T. Dufresne

Counsel for Amicus Curiae CClA

Supreme Court of Wisconsin

YASMEEN DANIEL, Individually, and as
Special Administrator of the Estate of Zina Daniel Haughton,
Plaintiff-Appellant,

TRAVELERS INDEMNITY COMPANY OF CONNECTICUT,
as Subrogee for Jalisco's LLC,
Intervening Plaintiff,

v.

ARMSLIST, LLC, an Oklahoma Limited Liability Company,
BRIAN MANCINI and JONATHAN GIBBON,
Defendants-Respondents-Petitioners,

BROC ELMORE, ABC INSURANCE CO., the fictitious name for an unknown insurance
company, DEF INSURANCE CO., the fictitious name for an unknown insurance company, and
ESTATE OF RADCLIFFE HAUGHTON, by his Special Administrator, Jennifer Valenti,
Defendants,

PROGRESSIVE UNIVERSAL INSURANCE COMPANY,
Intervening Defendant.

Appeal No. 2017AP344
Milwaukee County Circuit Court Case No. 2015CV8710

**APPENDIX TO BRIEF OF AMICUS CURIAE
COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION**

TABLE OF CONTENTS

Courtney v. Vereb,
2012 U.S. Dist. LEXIS 87286, 2012 WL 2405313 CCIA App. 1

Dryoff v. Ultimate Software Grp., Inc.,
2017 U.S. Dist. LEXIS 194524, 2017 WL 5665670 CCIA App. 7

Courtney v. Vereb

United States District Court for the Eastern District of Louisiana

June 21, 2012, Decided; June 25, 2012, Filed

CIVIL ACTION NO. 12-655 SECTION: A(4)

Reporter

2012 U.S. Dist. LEXIS 87286 *; 2012 WL 2405313

JOHN C. COURTNEY, PSY.D, MP versus DR.
BARTHOLOMEW VEREB AND ANGIE'S LIST,
INC.

Counsel: [*1] For John C Courtney, Psy.D., MP,
Plaintiff: Nakisha Ervin-Knott, LEAD
ATTORNEY, Justin I. Woods, Gainsburgh,
Benjamin, David, Meunier & Warshauer, New
Orleans, LA.

For Bartholomew Vereb, Dr., Defendant: Alan J.
Yacoubian, LEAD ATTORNEY, Neal J. Favret,
Johnson, Johnson, Barrios & Yacoubian, New
Orleans, LA.

For Angies List, Incorporated, Defendant: Kyle
Potts, LEAD ATTORNEY, David C. Coons,
Jaimme A. Collins, Adams & Reese, LLP (New
Orleans), New Orleans, LA.

Judges: JAY C. ZAINEY, UNITED STATES
DISTRICT JUDGE.

Opinion by: JAY C. ZAINEY

Opinion

ORDER AND REASONS

Before the Court is a **Motion to Dismiss (Rec. Doc. 8)** filed by Defendant Angie's List, Inc. pursuant to Fed. R. Civ. Proc. 12(b)(6), arguing that Plaintiff's claims are barred by the 1996 Communications Decency Act, 47 U.S.C. § 230 ("CDA"). Plaintiff Dr. John C. Courtney opposes the motion (**Rec. Doc. 12**). The motion, set for hearing on May 23, 2012, is before the Court on the

briefs without oral argument. For the following reasons, the motion is **GRANTED**.

I. BACKGROUND

This case stems from allegedly defamatory comments which Plaintiff Dr. John Courtney contends that Defendant Dr. Bartholomew Vereb made about him on a web page owned by Defendant Angie's List, Inc. [*2] Angie's List¹ describes itself as "an online community for members to find service companies and health care professionals in markets across the country. Members share their experiences about businesses/professionals from over 500 service categories, including doctors, carpet cleaners, handymen, landscapers, and caterers." See Rec. Doc. 8, p. 1. Angie's List advertises that it certifies its data before disseminating its reports to the public. It states on its website: "Before they're posted, all reviews are checked in order to guard against providers and companies that try to report on them or their competitors."²

Plaintiff alleges that, on June 2, 2009, Dr. Vereb "intentionally and maliciously, posted false and defamatory comments" about Dr. Courtney's professional services. See Plaintiff's Complaint at ¶¶ 10 and 19. According to the complaint, Dr. Vereb is a licensed physician, practicing psychiatry in Bradenton, Florida. He is also simultaneously licensed as a physician in Louisiana with a defined practice in psychiatry. Plaintiff states that, contrary

¹ <http://www.angieslist.com>.

² See <http://www.angieslist.com/howitworks.aspx>.

to Dr. Vereb's negative comments, Dr. Courtney had never [*3] met nor treated Dr. Vereb or anyone in Dr. Vereb's family.

Plaintiff purportedly became aware of the negative postings in "late December of 2011." *Id.* at ¶ 8. According to Plaintiff, he immediately contacted Angie's List via its online internal complaint form to request that it not disseminate Dr. Vereb's comments; however, Plaintiff received no response from Angie's List. Dr. Courtney alleges that he repeatedly advised Angie's List that the contents of the report were false and requested their removal over the course of several months. Plaintiff asserts that Angie's List eventually responded and recommended that Dr. Courtney post a response to Dr. Vereb's comments, which he did. Plaintiff continued to request the removal of the comments, however.

Plaintiff states that, on February 8, 2012, he received an e-mail from an Angie's List representative stating that Angie's List had removed Dr. Vereb's comments because it had discovered that Dr. Vereb operates in the same field as Dr. Courtney and Angie's List does not allow businesses to report on themselves or competitors.

Dr. Courtney subsequently filed suit against both Angie's List and Dr. Vereb in federal court. It is undisputed that [*4] this Court has subject matter jurisdiction over the instant matter pursuant to 28 U.S.C. § 1332 in that the claims asserted are against defendants with citizenship other than that of the plaintiff and because the amount in controversy exceeds \$75,000.000, exclusive of interests and costs.

Plaintiff's stated cause of action against Angie's List is that Angie's List, as "marketer, publisher, distributor and/or seller" of the information posted online, "owed a duty to the Plaintiff to certify its data and to verify the contents of any negative posting that purports to be factual statements." *Id.* at ¶¶ 28-29. Dr. Courtney alleges that Angie's List was negligent in failing to verify the truth of Dr. Vereb's reviews, which is "contrary to their own

stated policy of certifying data." *Id.* at ¶ 31. According to Dr. Courtney, "Angie's List's publication of the defamatory comments to third parties was malicious since it knew or should have known that the comments were false." *Id.* at ¶ 34. Dr. Courtney has requested a trial by jury, and seeks compensatory damages for past and future mental pain and suffering, past and future economic loss, past and future loss of earning capacity, as well as all [*5] general, special, incidental and consequential damages as may be proven at the time of trial. *Id.* at ¶ 35.

Angie's List brings this Motion to Dismiss (**Rec. Doc. 8**) based on the argument that Plaintiff's claims against it are precluded by the 1996 Communications Decency Act, 47 U.S.C. §230 ("CDA"). Having considered the record, the memoranda of counsel and the law, the Court has determined that dismissal is appropriate for the following reasons.

II. STANDARD OF REVIEW

Fed.R.Civ.P. 12(b)(6) authorizes a dismissal of a complaint for "failure to state a claim upon which relief can be granted." A 12(b)(6) motion should be granted only if it appears beyond doubt that the plaintiff could prove no set of facts in support of his claim that would entitle him to relief. See *Conley v. Gibson*, 355 U.S. 41, 45-46, 78 S. Ct. 99, 2 L. Ed. 2d 80 (1957). Before dismissal is granted, the court must accept all well-pleaded facts as true and view them in the light most favorable to the nonmovant. *Capital Parks, Inc. v. Southeastern Advertising and Sales Sys., Inc.*, 30 F.3d 627, 629 (5th Cir. 1994). A court need not, however, accept as true allegations that are conclusory in nature. *Kaiser Aluminum & Chem. Sales, Inc. v. Avondale Shipyards, Inc.*, 677 F.2d 1045, 1050 (5th Cir. 1982).

III. [*6] LAW & ANALYSIS

A. The Purpose and History of the CDA

To determine if Angie's List is immune from the claims brought against it by Plaintiff based on the provisions of the CDA, it is helpful to understand the rationale for the statute. By passing the CDA, Congress recognized the ever increasing role that the internet plays in worldwide communication. See Smith v. Intercosmos Media Group, Inc., 2002 U.S. Dist. LEXIS 24251, 2002 WL 31844907 at *2 (E.D.La., Dec. 17, 2002). Congress pointed to "the availability of educational and informational resources to our citizens" that the internet provides. Id. (quoting 47 U.S.C. § 230). It also hailed the internet as "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity" Id.

Congress saw the burgeoning internet as a benefit to all Americans. It also recognized that one reason the internet played such a beneficial role in American society was that the internet flourished "with a minimum of government regulation." Id. With the CDA, Congress made it an official policy of the United States "to promote the continued development of the internet and other interactive media, unfettered by federal [*7] or state regulation." Id. Clearly, the purpose of the CDA is to promote the free flow of information on the internet.

To ensure that web site operators and other interactive computer services would not be crippled by lawsuits arising out of third-party communications, the Act provides interactive computer services with immunity. Doe v. MySpace, Inc., 474 F.Supp.2d 843, 847 (W.D.Tex. 2007) (citing Dimeo v. Max, 433 F.Supp.2d 523, 528 (E.D.Pa. 2006) (internal citations and quotations omitted)). Congress provided immunity to "interactive computer service" providers for statements created by third parties but disseminated, and thus, published, by internet services. Unlike newspapers, radio stations, and other traditional media, under the CDA, websites may not be held liable for defamatory statements posted or sent through their services. R. L. Lackner,

Inc. v. Sanchez, 2005 U.S. Dist. LEXIS 40388, 2005 WL 3359356 at *2 (S.D.Tex., Dec. 9, 2005)(citing Blumenthal v. Drudge, 992 F.Supp. 44, 49 (D.D.C.1998)). However, individuals who create defamatory statements may be held liable even if the offending comments are published by posting on the internet. Id.

The CDA defines an "interactive computer service" as "any information [*8] 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." 47 U.S.C. § 230(f)(2). The statute identifies 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). The CDA immunizes providers and users of "interactive computer services" from liability for the information provided by a third party "information content provider." 47 U.S.C. § 230(c)(1).

One of the most important and oft-cited cases on CDA immunity to date is Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997). In Zeran, the victim of a vicious prank sued America Online, Inc. ("AOL") for failing to remove a false advertisement offering t-shirts featuring tasteless slogans related to the 1995 Oklahoma City bombing and instructing interested buyers to call the plaintiff to place an order. Zeran, 129 F.3d at 329. After receiving death threats from people who were outraged by the ad, Zeran [*9] learned of the prank and demanded that AOL remove the ad from its bulletin board and post a retraction. Id. AOL failed to remove the original ad, and the unidentified poster also posted several more ads listing the plaintiff's phone number. Id. A local radio station learned of the ads and encouraged its listeners to harass Zeran. Id. The volume and intensity of the threats became so severe that local police guarded Zeran's home to protect his safety. Id.

Zeran sued AOL for negligence because it failed to remove the ad after specific notice of its falsity and allowed the third party to post additional ads after Zeran had put AOL on notice of his harassment and bodily danger. The Fourth Circuit affirmed the dismissal of the claims on the pleadings, explaining that the CDA necessarily protects interactive computer services from liability even after they are notified of an allegedly defamatory or threatening post because the insupportable legal burden imposed by potential tort liability would undermine the CDA's goal of promoting speech on the Internet. *Id.* at 330. The Court explained that "[b]y its plain language, § 230 creates a federal immunity to any cause of action that would make [*10] service providers liable for information originating with a third-party user of the service." *Id.* In enacting the CDA, "Congress made a policy choice ... not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages." *Id.* at 330-31.

Three other federal courts of appeals have also held that the CDA immunizes computer service providers from liability for information that originates with third parties. *Doe v. Bates*, 2006 U.S. Dist. LEXIS 93348, 2006 WL 3813758 at *12 (E.D.Tex., Dec. 27, 2006)(citing *Carafano v. Metroplash.com Inc.*, 339 F.3d 1119, 1123 (9th Cir. 2003)(noting that the Ninth Circuit in *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003) had "joined the consensus developing across other courts of appeals that § 230(c) provides broad immunity for publishing content provided primarily by third parties"); *Green v. America Online*, 318 F.3d 465, 471 (3d Cir. 2003)(upholding immunity for the transmission of defamatory messages and a program designed to disrupt the recipient's computer); *Ben Ezra, Weinstein, & Co. v. America Online, Inc.*, 206 F.3d 980, 985-86 (10th Cir. 2000)(upholding immunity [*11] for the on-line provision of stock information even though AOL communicated frequently with the stock quote providers and had occasionally deleted stock

symbols and other information from its database in an effort to correct errors)).

B. Defendant May Claim Immunity Under the CDA

The CDA states 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). In *Smith v. Intercosmos Media Group, Inc.*, 2002 U.S. Dist. LEXIS 24251, 2002 WL 31844907 (E.D.La., Dec. 17, 2002), a court of this district employed a three-part test to determine whether a defendant could properly claim immunity under the CDA. Judge Berrigan held that, for purposes of CDA immunity: 1) the party claiming the immunity must be a provider or user of an interactive computer service; 2) the alleged defamatory statement must be made by a third party; 3) the defamation claim the party seeks immunity from must treat the interactive computer service as the publisher or speaker of the alleged defamatory statement. *Smith*, 2002 U.S. Dist. LEXIS 24251, 2002 WL 31844907 at *2.

Here, Plaintiff seeks to impose tort liability on a company that functions [*12] as an intermediary by providing a forum for the exchange of information between third party users. See *Doe v. Myspace*, 474 F.Supp. 2d at 848. In his opposition, Plaintiff contends that Angie's List cannot be granted immunity under the CDA because it is not merely just an "interactive computer service," but also provides copies of posted reviews to consumers upon request by telephone and fax. According to Plaintiff, Angie's List also operates as an "information content provider" because it requests that individuals, as part of their report generation process, respond to standard queries and provide additional content about the professional against whom they are reporting. In applying the three-part test to the facts of the instant case, the Court finds that Defendant Angie's List is entitled to CDA immunity for the following reasons.

1. Angie's List is an Interactive Computer Service

As stated *supra*, the CDA defines an interactive computer service as "any information service, system, or access software 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). The term "interactive computer service" [*13] differs from "information content provider," which 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." 47 U.S.C. § 230(f)(3). " Defendant Angie's List argues that it qualifies as an "interactive computer service" and thus meets the first prong of the test.

Plaintiff does not dispute that Angie's List offers an interactive exchange of information, but points out that members may be provided information on a service provider *by phone or fax*, as well as via the internet. According to Plaintiff, because Angie's List offers information by means other than online, it cannot claim the immunity protection of the CDA afforded to traditional interactive computer services. This argument is creative, but unsupported by the case law; Plaintiff did not provide, and the Court has been unable to locate, cases in which a website which offers users the option of receiving hard copies of online information via telephone or fax was deemed to be "not merely just an 'interactive computer service.'" See Rec. Doc. 12, p. 5. The Court finds that excluding websites which [*14] offer this type of additional service from the protection of the CDA would be contrary to the policy behind the statute, which was "to promote the continued development of the internet" by allowing it to expand "unfettered by federal or state regulation." 47 U.S.C. § 230.

2. Statements Were Made by a Third Party

Plaintiff readily admits that the allegedly defamatory statements were made by a third party, Defendant Dr. Vereb. Plaintiff's complaint states that the subject comments were "posted by Dr. Vereb," and that "Dr. Vereb intentionally and maliciously posted false and defamatory comments

concerning Plaintiff onto a national website to be viewed by all." Plaintiff Complaint, ¶¶ 10, 19.

However, Plaintiff also argues that Angie's List operates as an information content provider. Plaintiff asserts that "through its services, Angie's List requests that individuals, as part of their report generation process, provide additional content about the professional against whom they are report," and that they are therefore responsible for the allegedly defamatory content of Dr. Vereb's postings. Plaintiff Opposition, p. 7. Therefore, although Plaintiff admits that Angie's List is not solely responsible [*15] for creating the content complained of, Plaintiff argues that Angie's List is responsible, in part, for the "development of the content provided." *Id.*

However, Plaintiff fails to provide, and the Court has been unable to locate, binding case law establishing that a website's use of a questionnaire renders it a "content provider" of information provided in response to same. The allegedly defamatory statements objected to by Plaintiff were admittedly authored by Defendant Dr. Vereb; the Court finds no authority for Plaintiff's argument that Defendant Angie's List can be held liable for these statements in spite of the protective provisions of the CDA.

3. The Complaint Treats the Defendant as the Publisher of the Alleged Defamatory Statements

For CDA immunity from state and federal claims, the defendant must be treated as the publisher of the alleged defamatory statements. Plaintiff's complaint specifically alleges that Angie's List is the "publisher...of information to the general public searching for qualified medical services." Plaintiff Complaint ¶ 28. Therefore, the third part of the test is satisfied.

IV. CONCLUSION

The Court finds that Defendant Angie's List meets the three requirements [*16] for asserting CDA immunity against the claims brought against it by

Plaintiff. First, the defendant qualifies as an interactive service provider. Second, the defendant is not the source of the alleged defamatory statements. Third, the claim against the defendant treats the defendant as publisher of the alleged defamatory statements.

Accordingly,

IT IS ORDERED that the **Motion to Dismiss (Rec. Doc. 8)** filed by Defendant Angie's List, Inc. is hereby **GRANTED**. Plaintiff's claims against Angie's List are dismissed with prejudice.

New Orleans, Louisiana, this 21st day of June, 2012.

/s/ Jay C. Zainey

JAY C. ZAINY

UNITED STATES DISTRICT JUDGE

End of Document

Dyroff v. Ultimate Software Grp., Inc.

United States District Court for the Northern District of California, San Francisco Division

November 26, 2017, Decided; November 26, 2017, Filed

Case No. 17-cv-05359-LB

Reporter

2017 U.S. Dist. LEXIS 194524 *; 2017 WL 5665670

KRISTANALEA DYROFF, Plaintiff, v. THE ULTIMATE SOFTWARE GROUP, INC., Defendant.

Counsel: [*1] For Kristanalea Dyroff, individually and on behalf of the estate of Wesley Greer, deceased, Plaintiff: Sin-Ting Mary Liu, LEAD ATTORNEY, Aylstock Witkin Kreis & Overholtz PLLC, Alameda, CA; David F. Slade, PRO HAC VICE, Carney Bates & Pulliam, PLLC, Little Rock, AR.

For The Ultimate Software Group, Inc., Defendant: David Eugene Russo, Shawn Adrian Toliver, LEAD ATTORNEYS, Justin S. Kim, Lewis Brisbois Bisgaard & Smith LLP, San Francisco, CA; John Joseph Moura, LEAD ATTORNEY, Gilbert Kelly Crowley & Jennett LLP, Los Angeles, CA.

Judges: LAUREL BEELER, United States Magistrate Judge.

Opinion by: LAUREL BEELER

Opinion

ORDER GRANTING MOTION TO DISMISS

Re: ECF No. 13

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, [*2] 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 jurisdiction⁴ 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 immunity to website operators for third-party content on their website unless they

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.

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 [*3] 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, 70 Cal. Rptr. 3d 519 (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.

* * *

STATEMENT⁸

Experience Project⁹ is a (now dormant) social-network site consisting of various "online communities" or "groups" where users

⁷ *Id.* at 18.

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.

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 [*4] 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 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

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).

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).

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 [*5] 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 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 [*6] 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. 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 [*7] 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 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

¹⁸ *Id.* at 19 (¶ 44.)

¹⁹ *Id.* (¶ 45).

²⁰ *Id.* (¶ 46).

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).

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).

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 [*8] 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 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 [*9] — by the time of her son's death — Mr. Margenat-Castro's sales of fentanyl-laced heroin.³⁵

* * *

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, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (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, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (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 [*10] possibility

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).

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

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

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 website operators [*11] 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).

1.1.1 Immunity For Third-Party Content

First, website operators [*12] 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).

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

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

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). 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 [*13] 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,

³⁸The 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).

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 [*14] 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, Roommate³⁹ [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

³⁹The 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).

part."

Id. at 1166 (citing 47 U.S.C. § 230(f)(3)). Accordingly, the court held, "the fact that [third-party website] 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 [*15] 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 [*16] 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, [*17] 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]."⁴⁰ *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").

1.2.2 Does the Plaintiff Seek To Treat Ultimate Software as a [*18] 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. [*19] See, e.g., *Gonzalez v. Google, Inc.*, No. 16-cv-03282-DMR, 282 F. Supp. 3d 1150, 2017 U.S. Dist. LEXIS 175327, 2017 WL 4773366, at *10-11 (N.D. Cal. October 23, 2017) (rejecting the plaintiffs' argument that claims were not based 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 [*20] deem Ultimate Software to have "developed" the harmful content, at least in part, for two reasons:

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

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

(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* [*21] use of content that was generated in whole or in part by a third party."⁴⁵

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 [*22] "responsible, in whole or in part, for the creation or development of information." 47 U.S.C. §§ 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

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).

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)).

⁴⁹ *Id.* at 13-16 (citing *Roommates.com*, 521 F.3d at 1161-62, 1165, 1167-68, and *Anthony v. Yahoo! Inc.*, 421 F. Supp. 2d 1257, 1262-63

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 [*23] 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 (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 U.S. Dist. LEXIS 175327, 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 at 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* [*24]!, 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 [*25] 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, 410 U.S. App. D.C. 187 (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").

(N.D. Cal. 2006)).

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 [*26] 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. § 230(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 [*27] 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 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, [*28] 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. § 230(f)(3);

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

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

Roommates.com, 521 F.3d at 1174 n.37; *Barnes*, 570 F.3d at 1103; *Gonzalez*, 2017 U.S. Dist. LEXIS 175327, 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" information, even in part. 47 U.S.C. § 230(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, [*29] 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 [*30] 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.

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. GMAC*, 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 [*31] exercise due care, (2) breach of that duty, (3) causation, and (4) damages. *Merrill v. Navegar, Inc.*, 26 Cal. 4th 465, 110 Cal.

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

⁵³ *Id.*

Rptr. 2d 370, 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, 70 Cal. Rptr. 3d 519 (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, 80 Cal. Rptr. 2d 196 (1998)); *Thompson v. County of Alameda*, 27 Cal. 3d 741, 167 Cal. Rptr. 70, 614 P.2d 728, 732 (Cal. 1980); *Vasquez*, 118 Cal. App. 4th 269, 279, 12 Cal. Rptr. 3d 846 (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, 76 Cal. Rptr. 2d 809 (1998)); *accord Tarasoff v. Regents of Univ. of California*, 17 Cal. 3d 425, 131 Cal. Rptr. 14, 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*, 27 Cal. 4th 1112, 119 Cal. Rptr. 2d 709, 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 [*32] 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.*, 15 Cal. 3d 40, 123 Cal. Rptr. 468, 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, 110 Cal. Rptr. 2d 528, 28 P.3d 249 (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 [*33] 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*, 36 Cal. 4th 224, 30 Cal. Rptr. 3d 145, 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.*, 65 Cal. 2d 114, 52 Cal. Rptr. 561, 416 P.2d 793 (1966)). "The doctrine also extends to other types of special relationship[s] . . . including those between common carriers and

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

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, 252 Cal. Rptr. 11 (1988); see e.g., *Williams v. State of California*, 34 Cal. 3d 18, 192 Cal. Rptr. 233, 664 P.2d 137, 139 (Cal. 1983) (a factor supporting a special relationship is detrimental reliance by a person on another 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, 126 Cal. Rptr. 2d 213 (2002)) (citing *Rowland v. Christian*, 69 Cal. 2d 108, 70 Cal. Rptr. 97, 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 [*34] 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, 9 Cal. Rptr. 2d 216 (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), 2016 U.S.

Dist. LEXIS 192144, ECF No. 51 (C.D. Cal. Nov. 14, 2016). The court found no special relationship and thus no duty to warn. 2016 U.S. Dist. LEXIS 192144 at *11.

The plaintiff was an aspiring model who was a member of the networking website modelmayhem.com. 2016 U.S. Dist. LEXIS 192144 at *5. Two men — who were unaffiliated with the website — used the website to identify [*35] and lure victims (including the plaintiff) to Florida, where they drugged and raped the victims, filming the rapes for distribution as pornography videos. 2016 U.S. Dist. LEXIS 192144 at *3. 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. 2016 U.S. Dist. LEXIS 192144 at *4.

The case involved nonfeasance, not misfeasance. 2016 U.S. Dist. LEXIS 192144 at *8 (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. 2016 U.S. Dist. LEXIS 192144 at *5.

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 U.S. Dist. LEXIS 35562, 2017 WL 1304288, at *4 (D. Nev. Mar. 10, 2017). The plaintiff met and dated a man [*36] on Match.com and ended their relationship eight days later. 2017 U.S. Dist. LEXIS 35562, [WL] 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. 2017 U.S. Dist. LEXIS 35562, [WL] at *1-*3. Applying Nevada law, which is similar to California law, the court found no special relationship between Match.com and the plaintiff. 2017 U.S. Dist. LEXIS 35562, [WL] at *3-*4. The plaintiff was merely a paying subscriber, paid the fee, set up her profile, and was matched with the attacker. 2017 U.S. Dist. LEXIS 35562, [WL] at *3. The court concluded that the website had no special relationship with the plaintiff and thus no duty to warn her. 2017 U.S. Dist. LEXIS 35562, [WL] at *4.

These cases support the conclusion that a website has no "special relationship" with its users. Ms. Dyroff nonetheless contends that websites 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 [*37] 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), 2016 U.S. Dist. LEXIS 192144, ECF No. 51 at 6. It also "likely [would]

have a 'chilling effect' on the [I]nternet by opening the floodgates of litigation." 2016 U.S. Dist. LEXIS 192144 at *14 (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 the claim is that a social-network [*38] 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), 2016 U.S. Dist. LEXIS 192144, 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

⁵⁵ Opposition to Motion to Dismiss — ECF No. 15 at 24-26 (quoting *Taylor v. Centennial Bowl, Inc.*, 65 Cal. 2d 114, 52 Cal. Rptr. 561, 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 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.

recidivism — that a fellow member was a child molester. *Id.* (citing *Conti*, 235 Cal. App. 4th 1214, 186 Cal. Rptr. 3d 26 (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 [*39] serious inherited disease passed 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), 2016 U.S. Dist. LEXIS 192144, ECF No. 51 at 6 n.3 (citing *O'Hara v. Western Seven Trees Corp.*, 75 Cal. App. 3d 798, 142 Cal. Rptr. 487 (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, 142 Cal. Rptr. 487). 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 [*40] of fentanyl-laced

heroin.⁵⁷ The court holds that Ultimate Software'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. 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, 41 Cal. Rptr. 3d 389 (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.

Dated: [*41] November 26, 2017

/s/ Laurel Beeler

LAUREL BEELER

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

United States Magistrate Judge

End of Document