

United States District Court  
Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
San Francisco Division

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

Case No. 17-cv-05359-LB

**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.<sup>1</sup> Mr. Greer allegedly bought the drug from a drug dealer that he met online through their respective posts on Ultimate Software’s (now inactive) social-network website “Experience Project.” Ms. Dyroff asserts seven state claims: (1) Negligence, (2) Wrongful Death, (3) Premises Liability, (4) Failure to Warn, (5) Civil Conspiracy, (6) Unjust Enrichment, and (7) a violation of the Drug Dealer Liability Act (Cal. Health & Safety Code §§ 11700, *et seq.*).<sup>2</sup> She predicates Ultimate Software’s liability on its mining data from its users’ posts and using its proprietary

---

<sup>1</sup> 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.

<sup>2</sup> *Id.* at 26–37 (¶¶ 72–126).

United States District Court  
Northern District of California

1 algorithms to understand the posts and to make recommendations, which in this case steered Mr.  
2 Greer toward heroin-related discussion groups and the drug dealer who ultimately sold him the  
3 fentanyl-laced heroin.<sup>3</sup> Ultimate Software removed the action from state court based on diversity  
4 jurisdiction<sup>4</sup> and moved to dismiss all claims under Federal Rule of Civil Procedure 12(b)(6).<sup>5</sup>

5 For all claims except claim four, Ultimate Software asserts immunity under the  
6 Communications Decency Act, 47 U.S.C. § 230(c)(1).<sup>6</sup> Section 230(c)(1) provides immunity to  
7 website operators for third-party content on their website unless they are responsible, in whole or  
8 in part, for the creation or development of content. *Id.* §§ 230(c)(1) & (f)(3). The court dismisses  
9 the claim because Ultimate Software is immune under § 230(c)(1). Its “[content]-neutral tools”  
10 facilitated communication but did not create or develop it. *Fair Hous. Council of San Fernando*  
11 *Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1167–69 (9th Cir. 2008) (en banc).

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

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

21 \* \* \*

22  
23  
24  
25 <sup>3</sup> Opposition to Motion to Dismiss – ECF No. 15 at 12.

26 <sup>4</sup> Notice of Removal – ECF No. 1 at 1–3.

27 <sup>5</sup> Motion to Dismiss – ECF No. 13-1.

28 <sup>6</sup> *Id.* at 8.

<sup>7</sup> *Id.* at 18.

1 **STATEMENT**<sup>8</sup>

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

8 Thus, Experience Project allowed users to register on the site with anonymous user names and  
9 thereafter join or start groups based on their experiences or interests, such as “I like dogs,” “I have  
10 lung cancer,” “I’m going to Stanford,” or “I Love Heroin,” and to post and discuss their personal  
11 experiences and interests to those groups.<sup>12</sup> After a user established an account and joined a group,  
12 the user could ask questions or answer questions posed by other members.<sup>13</sup> Ultimate Software,  
13 using advanced data-mining algorithms, analyzed the posts and other user data to glean  
14 information, including the underlying intent and emotional state of the users.<sup>14</sup> Ultimate Software  
15 used this information both for its own commercial purposes (such as selling data sets to third  
16 parties) and to steer Experience Project users to other groups on its website through its proprietary  
17 recommendation functionality.<sup>15</sup> It also utilized email and other “push” notifications to alert users  
18  
19

20 <sup>8</sup> The allegations in the “Statement” are from the plaintiff’s complaint. *See* Compl. – ECF No. 1-1.

21 <sup>9</sup> The plaintiff initially named Experience Project and Kanjoya, Inc. as additional defendants. Comp. –  
22 ECF No. 1-1. In its notice of removal, Ultimate Software explained that it acquired the website  
23 Experience Project from Kanjoya, which now is a wholly owned subsidiary of Ultimate Software.  
24 Notice of Removal – ECF No. 1; Stipulation – ECF No. 18. The parties then stipulated to dismiss  
25 Experience Project and Kanjoya. Stipulation – ECF No. 18. Ultimate Software thus is the only  
26 defendant.

27 <sup>10</sup> Compl. – ECF No. 1-1 at 6 (¶ 12), 8 (¶ 18).

28 <sup>11</sup> *Id.* at 16 (¶ 36).

<sup>12</sup> *Id.* at 3 (¶ 2), 8 (¶ 18), 20 (¶ 54).

<sup>13</sup> *Id.* at 9 (¶ 21).

<sup>14</sup> *Id.* at 3 (¶ 2).

<sup>15</sup> *Id.* at 3 (¶ 2) and 9 (¶ 22).

1 when a new post or response occurred.<sup>16</sup> As of May 2016, the website had over sixty-seven  
2 million “experiences shared.”<sup>17</sup>

3 In 2007, when he was a college student, Mr. Greer suffered a knee injury. During his recovery,  
4 he was prescribed opioid painkillers and became addicted, first to opioids and then to heroin.<sup>18</sup> He  
5 began treatment in 2011, completing five separate rehab programs, but he relapsed each time.<sup>19</sup> By  
6 2013, he had completed a faith-based program in Florida, remained clean, and continued living  
7 and working there.<sup>20</sup> In January 2015, the program was unable to hire him, and he left to run a  
8 halfway house. He was concerned that the drug-seeking environment there endangered his  
9 sobriety, and in February 2015, he moved home to Brunswick, Georgia, to live with his mother  
10 and stepfather and help them renovate their house.<sup>21</sup>

11 In August 2015, Mr. Greer conducted a Google search to find heroin, and he was directed to  
12 the defendant’s website “Experience Project.”<sup>22</sup> He created an account with Experience Project,  
13 purchased “tokens” (which enabled him to post questions to other users), and posted to a group  
14 titled “where can i score heroin in jacksonville, fl.”<sup>23</sup>

15 On August 17, 2015, Experience Project sent an email to Mr. Greer notifying him that  
16 “Someone posted a new update to the question ‘where can i score heroin in jacksonville, fl,’” and  
17 providing a hyperlink and a URL directing him to the update.<sup>24</sup> This update (or a similar one)  
18 alerted Mr. Greer that another Experience Project user, Hugo Margenat-Castro, an Orlando-based  
19 drug dealer, had responded to Mr. Greer’s post. Mr. Greer was able to obtain his phone number  
20

21  
22 <sup>16</sup> *Id.* at 5 (¶ 8), 20 (¶ 52), 25–26 (¶ 70).

23 <sup>17</sup> *Id.* at 9 (¶ 20).

24 <sup>18</sup> *Id.* at 19 (¶ 44.)

25 <sup>19</sup> *Id.* (¶ 45).

26 <sup>20</sup> *Id.* (¶ 46).

27 <sup>21</sup> *Id.* (¶¶ 47–48).

28 <sup>22</sup> *Id.* at 20 (¶ 49).

<sup>23</sup> *Id.* at 20 (¶¶ 49–51).

<sup>24</sup> *Id.* at 20 (¶ 52).

1 through Experience Project.<sup>25</sup> Mr. Greer called Mr. Margenat-Castro, and in the early hours of  
2 August 18, 2015, drove from Brunswick, Georgia, to Orlando, Florida, where he bought fentanyl-  
3 laced heroin from Mr. Margenat-Castro. He then returned to Brunswick.<sup>26</sup> On August 19, 2015,  
4 Mr. Greer died from fentanyl toxicity.<sup>27</sup>

5 In numerous earlier posts on Experience Project, Mr. Margenat-Castro offered heroin for sale  
6 in groups such as “I love Heroin” and “heroin in Orlando.” He actually sold heroin mixed with  
7 fentanyl (“a fact that he hid in his posts” and “misrepresented as heroin”). Fentanyl is a synthetic  
8 opioid that is fifty times stronger than heroin.<sup>28</sup>

9 Before Mr. Greer’s death, Mr. Margenat-Castro regularly used Experience Project to sell a  
10 mixture of heroin and fentanyl. Based on his activity on Experience Project, law-enforcement  
11 agencies conducted “controlled buys” of heroin from Mr. Margenat-Castro on March 31, 2015,  
12 and June 24, 2015, and Mr. Margenat-Castro was arrested on April 1, 2015, and June 25, 2015, for  
13 possession with intent to sell fentanyl, among other drugs, stemming from his sale of drugs on  
14 Experience Project’s website.<sup>29</sup> Officers made another controlled buy from Mr. Margenat-Castro  
15 on September 3, 2015. They tied him to his Experience Project handle “Potheadjuice,” confirmed  
16 through a toxicology report that the substance contained fentanyl, and obtained an arrest warrant  
17 on October 7, 2015.<sup>30</sup> In his March 2017 plea agreement, Mr. Margenat-Castro estimated that he  
18 sold ten bags of fentanyl-laced heroin every day (seven days a week) between January 2015 and  
19 October 2015 via Experience Project. He estimated selling roughly 1,400 bags of heroin laced  
20 with fentanyl.<sup>31</sup> Ms. Dyroff contends that by August 17, 2015, when her son bought the drugs  
21  
22

---

23 <sup>25</sup> *Id.* at 20–21 (¶¶ 53–55).

24 <sup>26</sup> *Id.* at 20–21 (¶¶ 54–55, 57).

25 <sup>27</sup> *Id.* at 21 (¶ 57).

26 <sup>28</sup> *Id.* at 5 (¶¶ 7–8), 20 (¶ 54), 22–23 (¶ 61).

27 <sup>29</sup> *Id.* at 22–23 (¶¶ 61, 63).

28 <sup>30</sup> *Id.* at 24 (¶ 67).

<sup>31</sup> *Id.* at 21–22 (¶ 58), 23–24 (¶ 64).

1 from Mr. Margenat-Castro, Ultimate Software had actual or constructive knowledge of Mr.  
2 Margenat-Castro’s trafficking fentanyl-laced heroin on Experience Project.<sup>32</sup>

3 Ms. Dyroff alleges that Ultimate Software operated Experience Project in an unlawful manner  
4 that facilitated extensive drug trafficking between drug dealers and drug buyers, even providing  
5 “reviews” of drug dealers who trafficked on Experience Project’s website.<sup>33</sup> Specifically, she  
6 alleges that Ultimate Software:

- 7 (1) allowed its Experience Project users to anonymously traffic in illegal deadly  
8 narcotics;
- 9 (2) allowed users to create groups dedicated to the sale and use of such illegal  
10 narcotics;
- 11 (3) steered users to “additional” groups dedicated to the sale of such narcotics  
12 (through the use of its advanced data-mining algorithms to manipulate and  
13 funnel vulnerable individual users to harmful drug trafficking groups on  
14 Experience Project’s website);
- 15 (4) sent users emails and other push notifications of new posts in those groups  
16 related to the sale of deadly narcotics;
- 17 (5) allowed Experience Project users to remain active account holders despite (a)  
18 the users’ open drug trafficking on Experience Project’s website, (b) Ultimate  
19 Software’s knowledge of this (including knowledge acquired through its  
20 proprietary data-mining technology, which allowed it to analyze and understand  
21 its users’ drug-trafficking posts) and (c) multiple law-enforcement actions  
22 against users related to their drug dealing on the Experience Project website;
- 23 (6) exhibited general and explicit antipathy towards law enforcement’s efforts to  
24 curb illegal activity on Experience Project’s website;<sup>34</sup> and
- 25 (7) received numerous information requests, subpoenas, and warrants from law  
26 enforcement and should have known about drug trafficking on its site by its  
27 users, including — by the time of her son’s death — Mr. Margenat-Castro’s  
28 sales of fentanyl-laced heroin.<sup>35</sup>

\* \* \*

<sup>32</sup> *Id.* at 22–24 (¶¶ 61, 63, 66).

<sup>33</sup> *Id.* at 13 (¶ 31), 25–26 (¶ 70), 26–27 (¶ 73), 27 (¶ 75).

<sup>34</sup> *Id.* at 26–27 (¶ 73), 3–4 (¶¶ 2–3), 16–17 (¶ 38).

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

**GOVERNING LAW**

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

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

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

\* \* \*

United States District Court  
Northern District of California

**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).<sup>36</sup> The CDA provides that website operators are immune from liability for third-party “information” (such as the posts here) unless the website operator “is responsible, in whole or in part, for the creation or development of the information.” *Id.* §§ 230(c)(1) & (f)(3). The plaintiff contends that Ultimate Software developed third-party information (or content) here by mining data from its users’ posts and using its proprietary algorithms to understand the posts and to make recommendations, which in this case steered Mr. Greer toward heroin-related discussions and the drug dealer who sold him fentanyl-laced heroin.<sup>37</sup> 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).

<sup>36</sup> Motion to Dismiss – ECF No. 13-1 at 8–15.

<sup>37</sup> Opposition to Motion to Dismiss – ECF No. 15 at 12.



### 1.1.1 Immunity For Third-Party Content

1 First, website operators generally are immune from liability from third-party posts. *Id.* Under  
2 the CDA, “[n]o provider or user of an *interactive computer service* shall be treated as the publisher  
3 or speaker of any information provided by *another information content provider.*” 47 U.S.C. §  
4 230(c)(1) (emphasis added). Moreover, “no [civil] liability may be imposed under any State or  
5 local law that is inconsistent” with § 230(c)(1). *Id.* § 230(e)(3).  
6

7 The most common “interactive computer services” are websites. *Roommates.com*, 521 F.3d at  
8 1162 n.6.<sup>38</sup> The CDA defines an “information content provider” as “any person or entity that is  
9 responsible, in whole or in part, for the creation or development of information provided through  
10 the Internet or any other interactive computer service.” 47 U.S.C. § 230(f)(3).

11 In general, then, § 230(c)(1) “protects websites from liability for material posted on the[ir]  
12 website[s] by someone else.” *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 850 (9th Cir. 2016).  
13 More specifically, § 230(c)(1) “immunizes providers of interactive computer services against  
14 liability arising from content created by third parties.” *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1265  
15 (2016) (quoting *Roommates.Com*, 521 F.3d at 1162). Section 230(c) thus “overrides the traditional  
16 treatment of publishers, distributors, and speakers under statutory and common law.” *Batzel v.*  
17 *Smith*, 333 F.3d 1018, 1026 (9th Cir. 2003). “The prototypical service qualifying for [CDA]  
18 immunity is an online messaging board (or bulletin board) on which Internet subscribers post  
19 comments and respond to comments posted by others.” *Kimzey*, 836 F.3d at 1266 (quoting *FTC v.*  
20 *Accusearch Inc.*, 570 F.3d 1187, 1195 (10th Cir. 2009)).

### 1.1.2 No Immunity for Websites That Create or Develop Content

21 But if a website operator “is responsible, in whole or in part, for the creation or development  
22 of information” on its website, then it is an “information content provider,” and it does not have  
23 immunity from liability for that information. 47 U.S.C. §§ 230(c)(1) & (f)(3); *Roommates.com*,  
24

25  
26  
27 <sup>38</sup> The definition “interactive computer service” is “any information service, system, or access software  
28 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).

1 521 F.3d at 1165. As the Ninth Circuit has explained, the CDA “does not declare ‘a general  
2 immunity from liability deriving from third-party content.’” *Internet Brands*, 824 F.3d at 852  
3 (quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100 (9th Cir. 2009)). Nor was it “meant to create  
4 a lawless no-man’s land on the Internet.” *Roommates.com*, 521 F.3d at 1164.

5 In *Roommates.com*, the Ninth Circuit considered whether Roommates.com created content,  
6 found that it did (at least “in part”), and concluded that it was not entitled to § 230(c)(1) immunity  
7 for the content that it created. 521 F.3d at 1165. Roommates.com operated a website that matched  
8 people renting rooms to people looking for a place to live. *Id.* at 1161. It required subscribers to  
9 create profiles and answer questions — about themselves and preferences in roommates —  
10 regarding criteria including sex, sexual orientation, and whether they would bring children to the  
11 household. *Id.* at 1161. The Fair Housing Councils of the San Fernando Valley and San Diego  
12 sued Roommates.com, alleging that it violated the federal Fair Housing Act and California  
13 housing-discrimination laws. *Id.* at 1162. Roommates.com asserted that it had immunity under §  
14 230(c)(1).

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

17 By requiring subscribers to provide the information as a condition of accessing its  
18 service, and by providing a limited set of pre-populated answers, Roommate<sup>39</sup>  
19 [became] much more than a passive transmitter of information provided by others;  
20 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.’”

21 *Id.* at 1166 (citing 47 U.S.C. § 230(f)(3)). Accordingly, the court held, “the fact that [third-  
22 party website] users are information content providers does not preclude [the website  
23 itself] from *also* being an information content provider by helping ‘develop’ at least ‘in  
24 part’ the information” at issue. *Roommates.com*, 521 F.3d at 1165 (emphasis in the  
25 original). This means that

26 [a] website operator can be both a service provider and a content provider: If it

27 \_\_\_\_\_  
28 <sup>39</sup> The opinion refers to “Roommate” (as opposed to the plural Roommates, which is the spelling in the  
case caption and in the company’s name Roommates.com).

1 passively displays content that is created entirely by third parties, then it is only a  
2 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.”

3 *Id.* at 1162 (quoting 47 U.S.C. § 230(f)(3)). “Thus, a website may be immune from liability for  
4 some of the content it displays to the public but be subject to liability for other content.” *Id.* at  
5 1162–63. As the court summed up, “[t]he CDA does not grant immunity for inducing third parties  
6 to express illegal preferences. Roommate’s own acts — posting the questionnaire and requiring  
7 answers to it — are entirely its doing and thus section 230 of the CDA does not apply to them.  
8 Roommate is entitled to no immunity.” *Id.* at 1165.

9 By contrast, the court immunized Roommates.com from liability for statements that  
10 subscribers independently displayed in an “Additional Comments” section of their profile. *Id.* at  
11 1173–74. Roommates.com prompted subscribers to “personalize your profile by writing a  
12 paragraph or two describing yourself and what you are looking for in a roommate.” *Id.* at 1173.  
13 “[S]ubscribers provide[d] a variety of provocative and often very revealing answers,” such as their  
14 preferences for roommates’ sex, sexual orientation, and religion. *Id.* Roommates.com published  
15 the statements as written, did not provide guidance about content, and did not “urge subscribers to  
16 input discriminatory preferences.” *Id.* at 1173–74. The court held that Roommates.com was “not  
17 responsible, in whole or in part, for the development of this content, which comes entirely from  
18 subscribers and is passively displayed by Roommate.” *Id.* at 1174. “Without reviewing every post,  
19 Roommate would have no way to distinguish unlawful discriminatory preferences from perfectly  
20 legitimate statements.” *Id.* Moreover, there could be no “doubt that this information was tendered  
21 to Roommate for publication online.” *Id.* “This,” the Ninth Circuit held, “is precisely the kind of  
22 situation for which section 230 was designed to provide immunity.” *Id.*

23 As an illustration of the difference between publishing third-party content (entitling the  
24 website operator to immunity) and developing content (resulting in no immunity), the Ninth  
25 Circuit distinguished Roommates.com’s search function from generic search engines. *Id.* at 1167.  
26 Roommates.com steered users based on discriminatory criteria, thereby limiting search results and  
27 forcing users to participate in its discriminatory process. *Id.* By contrast, generic search engines  
28 such as Google, Yahoo!, and MSN “do not use unlawful criteria to limit the scope of the

1 searches[.]. . . [are not] designed to achieve illegal ends [unlike Roommates.com’s alleged search  
 2 function, and thus] . . . play no part in the ‘development’ of any unlawful searches.” *Id.* at 1167.  
 3 The court concluded that “providing neutral tools to carry out what may be unlawful or illicit  
 4 [activities] does not amount to ‘development’ for purposes of the immunity exception.” *Id.* at  
 5 1168–69.

### 6 **1.1.3 Three-Element Test for Immunity Under § 230(c)(1)**

7 Separated into its elements, § 230(c)(1) protects from liability “(1) a provider or user of an  
 8 interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action,  
 9 as a publisher or speaker (3) of information provided by another information content provider  
 10 [here, Mr. Margenat-Castro].” *Kimzey*, 836 F.3d at 1268 (quoting *Barnes*, 570 F.3d at 1100–01).

## 11 **1.2 Application Of the Three-Element Test To Ms. Dyroff’s Claims**

### 12 **1.2.1 Is Ultimate Software a Provider of an Interactive Computer Service?**

13 The first element is whether Experience Project is an “interactive computer service.” It is  
 14 undisputed that it is.<sup>40</sup> *See Roommates.com*, 521 F.3d at 1162 (websites are the most common  
 15 “interactive computer services”).

### 16 **1.2.2 Does the Plaintiff Seek To Treat Ultimate Software as a Publisher?**

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

23 The issue here is whether plaintiffs can plead around § 230(c)(1) immunity by basing their  
 24 claims on the website’s tools, rather than the website operator’s role as a publisher of the third-  
 25 party content. The Ninth Circuit has held that what matters is whether the claims “inherently  
 26

27 <sup>40</sup> *See, e.g.*, Compl. – ECF No. 1-1 at 8 (¶ 18).

28 <sup>41</sup> Opposition to Motion to Dismiss – ECF No. 15 at 12.

1 require[] the court to treat the defendant as the ‘publisher or speaker’ of content provided by  
2 another.” *Barnes*, 570 F.3d at 1102. If they do, then § 230(c)(1) precludes liability. *Id.*; accord  
3 *Airbnb, Inc. v. City & County of San Francisco*, 217 F.Supp.3d 1066, 1074 (2016) (citing *Barnes*,  
4 570 F.3d at 1102).

5 In similar cases, courts have rejected plaintiffs’ attempts to plead around immunity by basing  
6 liability on a website’s tools. See, e.g., *Gonzalez v. Google, Inc.*, No. 16-cv-03282-DMR, 2017  
7 WL 4773366, at \*10–11 (N.D. Cal. October 23, 2017) (rejecting the plaintiffs’ argument that  
8 claims were not based Google’s publishing third-party content from ISIS but instead were based  
9 on Google’s “provid[ing] ISIS followers with access to powerful tools and equipment to publish  
10 their own content”); *Fields v. Twitter*, 217 F. Supp. 3d 1116, 1121–22 (N.D. Cal. 2016), *appeal*  
11 *docketed*, No. 16-17165 (9th Cir. Nov. 25, 2016) (rejecting the plaintiffs’ argument that their  
12 claims were not based on Twitter’s publishing third-party content by ISIS but instead were based  
13 on Twitter’s allowing ISIS members to sign up for Twitter accounts).

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

### 16 **1.2.3 Is the Harmful Content “Third-Party Content”?**

17 The third element is whether the content is third-party content. A third party — Mr. Margenat-  
18 Castro — posted on Experience Project. The issue is whether his posts and other allegedly harmful  
19 content are third-party content, which means that § 230(c)(1) bars the claims against Ultimate  
20 Software, or whether Ultimate Software “is responsible, in whole or in part, for the creation or  
21 development of the information,” which means that § 230(c)(1) does not bar the claims. 47 U.S.C.  
22 § 230(c)(1) & (f)(3).

23 Ms. Dyroff contends that the court should deem Ultimate Software to have “developed” the  
24 harmful content, at least in part, for two reasons: (1) its tools, design, and functionality abetted the  
25 content, at least in part, by recommending heroin-related discussions and steering Mr. Greer to Mr.  
26 Margenat-Castro’s posts; and (2) Ultimate Software is not merely a passive conduit for its users’  
27 posts because it knew that Experience Project was an online market for drug dealers and users, and  
28

1 it shielded the bad actors through its anonymity policies and antipathy to law enforcement.<sup>42</sup>

### 2 **1.2.3.1 Ultimate Software’s Use of Tools to Develop Content**

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

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

---

22 <sup>42</sup> *Id.* at 13–23.

23 <sup>43</sup> *Id.* at 17.

24 <sup>44</sup> *Id.* at 13 (citing *Roommates.com*, 521 F.3d at 1168).

25 <sup>45</sup> *Id.* (citations omitted).

26 <sup>46</sup> *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)).

27 <sup>47</sup> *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).

28 <sup>48</sup> *Id.* at 10 (citing Compl. – ECF No. 1-1 at 11–16 (¶¶ 26–35)).

1 The ordinary rule is that Ultimate Software is immune from liability for third-party content on  
2 its website unless it is “responsible, in whole or in part, for the creation or development of  
3 information.” 47 U.S.C. §§ 230(c)(1) & (f)(3). Here, only third parties posted information on  
4 Experience Project, and the website operator did not solicit unlawful information or otherwise  
5 create or develop content. Ultimate Software is not an “information content provider” merely  
6 because its content-neutral tools (such as its algorithms and push notifications) steer users to  
7 unlawful content. *Roommates.com*, 521 F.3d at 1167. The following points support this  
8 conclusion.

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

13 In *Roommates.com*, the website operator created a questionnaire, provided a limited set of pre-  
14 populated (and unlawful) answers as a condition of accessing the website and its services, and  
15 steered users based on the pre-populated answers. 521 F.3d at 1166–67. By these acts,  
16 Roommates.com “[became] much more than a passive transmitter of information provided by  
17 others; it [became] the developer, at least in part, of that information. And section 230 provides  
18 immunity only if the interactive computer service does not ‘creat[e] or develop[.]’ the information  
19 ‘in whole or in part.’” *Id.* at 1166 (quoting 47 U.S.C. § 230(f)(3)). By contrast, here, Ultimate  
20 Software did not solicit unlawful content from its third-party users and merely provided content-  
21 neutral social-network functionalities — recommendations and notifications about posts.  
22 “Providing neutral tools for navigating websites is fully protected by CDA immunity, absent  
23 substantial affirmative conduct on the part of the website creator promoting the use of such tools  
24 for unlawful purposes.” *Id.* at 1174 n.37; accord *Gonzalez*, 2017 WL 4773366, at \*11 (rejecting  
25 claim that Google was liable because YouTube’s website “functionality” purportedly facilitated  
26

27 \_\_\_\_\_  
28 <sup>49</sup> *Id.* at 13–16 (citing *Roommates.com*, 521 F.3d at 1161–62, 1165, 1167–68, and *Anthony v. Yahoo!*,  
421 F. Supp. 2d 1257, 1262–63 (N.D. Cal. 2006)).



1 ISIS’s communication of its message, which resulted in great harm); *Cohen v. Facebook, Inc.*, 252  
2 F. Supp. 3d 140, 158 (E.D.N.Y. May 18, 2017) (rejecting claim that Facebook provided a tool to  
3 support terrorist organizations); *Fields*, 217 F. Supp. 3d 1120–23 (rejecting claim that Twitter  
4 provided ISIS with material support by permitting it to sign up for accounts). Ms. Dyroff does not  
5 plausibly allege that Ultimate Software “promoted the use of [its neutral] tools for unlawful  
6 purposes.” *Roommates.com*, 521 F.3d at 1174 n.37.

7 Similarly, Ms. Dyroff relies on *Anthony v. Yahoo!*, but does not allege facts comparable to  
8 those in that case. Yahoo! allegedly created fake user profiles and sent them — along with actual  
9 user profiles of former subscribers — to current website users to try to persuade them to renew  
10 their lapsed subscriptions to Yahoo’s online dating service. 421 F. Supp. 2d at 1262. Assuming the  
11 allegations to be true for its Rule 12(b)(6) inquiry, the court held that Yahoo! was not immune  
12 under § 230(c)(1) for two reasons. *Id.* First, Yahoo! created content in the form of the false  
13 profiles and thus was an “information content provider.” *Id.* at 1262–63. Second, with actual  
14 knowledge of the false profiles — including those of former users — Yahoo! used the content to  
15 (allegedly) commit fraud and thus was responsible for its misrepresentations. *Id.* (collecting cases  
16 on § 230(c)(1) immunity). By contrast, here, Ultimate Software did not create or use unlawful  
17 content and merely provided its neutral social-network functionalities.

18 Second, it is the users’ voluntary inputs that create the content on Experience Project, not  
19 Ultimate Software’s proprietary algorithms. *See, e.g., Kimzey*, 836 F.3d at 1268–70 (Yelp!’s “star-  
20 rating system is best characterized as the kind of ‘neutral tool[]’ operating on ‘voluntary inputs’  
21 that we determined that does not amount to content development or creation in *Roommates.com*,  
22 521 F.3d at 1172.”). Moreover, even if a tool “‘facilitates the expression of [harmful or unlawful]  
23 information,’” it is considered neutral “so long as users ultimately determine what content to post,  
24 such that the tool merely provides ‘a framework that could be utilized for proper or improper  
25 purposes.’” *Goddard v. Google, Inc.*, 640 F. Supp. 2d 1193, 1195 (N.D. Cal. 2009) (rejecting  
26 claim that Google’s “Keyword Tool” — which provides options that advertisers can adopt or  
27 reject at their discretion — created liability for subsequent postings by the advertisers of false or  
28 misleading advertisements) (citing *Roommates.com*, 521 F.3d at 1172); *Carafano*, 339 F.3d at



1 1121, 1124; *see also Klayman v. Zuckerberg*, 753 F.3d 1354, 1358 (D.C. Cir. 2014) (“a website  
2 does not create or develop content when it merely provides a neutral means by which third parties  
3 can post information of their own independent choosing online”).

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

10 The court follows these cases and holds that the Experience Project website’s alleged  
11 functionalities — including its user anonymity, algorithmic recommendations of related groups,  
12 and the “push” e-mail notification of posts and responses — are content-neutral tools.  
13 *Roommates.Com*, 521 F.3d at 1168–69. They do not make Ultimate Software an “information  
14 content provider” that “is responsible, in whole or in part, for the creation or development of  
15 information provided through the Internet or any other interactive computer service,” even if the  
16 tools were used to facilitate unlawful activities on the site. *See* 47 U.S.C. § 270(f)(3);  
17 *Roommates.com*, 521 F.3d at 1174 n.37; *Carafano*, 339 F.3d at 1123. In sum, Ultimate Software is  
18 immune under § 230(c)(1) as a publisher of content created entirely by third-party users.

### 19 **1.2.3.2 Online Market For Drug Trafficking and Shielding Bad Actors**

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

27  
28 <sup>50</sup> *Id.* at 18; *see also* Compl. – ECF No. 1-1 at 17-19 (¶¶ 39–42).

1 From day one, the privacy of our users has been paramount and we have never  
2 allowed names, phone numbers, or addresses. This approach bucked every trend,  
3 and challenged our ability to build an advertising-based business, but we  
4 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.

5 But, there are deeper, and more troubling trends than formats. Online anonymity, a  
6 core part of EP, is being challenged like never before. Governments and their  
7 agencies are aggressively attacking the foundations of internet privacy with a  
deluge of information requests, subpoenas, and warrants. We, of course, always  
support proper law enforcement efforts, but the well-documented potential for even  
abuse, even if unintentional, is enormous and growing.<sup>51</sup>

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

12 Moreover, as the analysis in the last section establishes, Ultimate Software's functionalities are  
13 neutral tools that do not transform Ultimate Software into an "information content provider," even  
14 if the tools were used to facilitate unlawful activities on the site. 47 U.S.C. § 270(f)(3);  
15 *Roommates.com*, 521 F.3d at 1174 n.37; *Barnes*, 570 F.3d at 1103; *Gonzalez*, 2017 WL 4773366,  
16 at \*10. Ultimate Software's policy about anonymity may have allowed illegal conduct, and the  
17 neutral tools facilitated user communications, but these website functionalities do not "create" or  
18 "develop" information, even in part. 47 U.S.C. § 270(f)(3); *Roommates.com*, 521 F.3d at 1174  
19 n.37; *Carafano*, 339 F.3d at 1123. And they do not show that Ultimate Software engaged in  
20 "substantial affirmative conduct . . . promoting the use of [the] tools for unlawful purposes."  
21 *Roommates.com*, 521 F.3d at 1167–68, 1174 n.37. Liability requires more than "neutral tools." *Id.*

22 As the Ninth Circuit concluded in *Roommates.com*: “

23 Websites are complicated enterprises, and there will always be close cases where a  
24 clever lawyer could argue that something the website operator did encouraged the  
25 illegality. Such close cases, we believe, must be resolved in favor of immunity, lest  
26 we cut the heart out of section 230 by forcing websites to . . . fight[] off claims that  
27 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

28 <sup>51</sup> Compl. – ECF No. 1-1 at 17-18 (¶ 41) (emphasis omitted).

1 enhancement by implication or development by inference... [,] section 230 must be  
2 interpreted to protect websites not merely from ultimate liability, but from having  
to fight costly and protracted legal battles.

3 521 F.3d at 1174–75.

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

## 6 7 **2. Count Four: Failure to Warn**

8 In claim four, Ms. Dyroff contends that Ultimate Software had a duty to warn Mr. Greer that  
9 Mr. Margenat-Castro was selling fentanyl-laced heroin via the Experience Project website.<sup>52</sup>

10 Ultimate Software moves to dismiss the claim on the grounds that (1) it had no “special  
11 relationship” with Mr. Greer or created any risks that gave rise to a duty to warn him, and (2) Mr.  
12 Greer assumed the risk of buying drugs from an anonymous Internet drug dealer.<sup>53</sup> The CDA does  
13 not preclude a failure-to-warn claim. *Internet Brands*, 824 F.3d at 849–54.

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

### 17 **2.1 Duty to Warn: Special Relationship — Nonfeasance (Failure to Act)**

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

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

26  
27 \_\_\_\_\_  
<sup>52</sup> Motion to Dismiss – ECF No. 13-1 at 18–21; Reply – ECF No. 16 at 18–20.

28 <sup>53</sup> *Id.*

1 The elements of a negligence claim are (1) the existence of a duty to exercise due care, (2)  
2 breach of that duty, (3) causation, and (4) damages. *Merrill v. Navegar, Inc.*, 28 P.3d 116, 139  
3 (Cal. 2001). A duty to exercise due care is an “obligation to conform to a certain standard of  
4 conduct for the protection of others against unreasonable risks.” *McGarry v. Sax*, 158 Cal. App.  
5 4th 983, 994 (2008) (quotation omitted).

6 “The existence of a legal duty to use reasonable care in a particular factual situation is a  
7 question of law for the court to decide.” *McGarry*, 158 Cal. App. 4th at 994 (quoting *Adams v.*  
8 *City of Fremont*, 68 Cal. App. 4th 243, 265 (1998)); *Thompson v. County of Alameda*, 27 P.2d  
9 728, 732 (Cal. 1980); *Vasquez*, 118 Cal. App. 4th 269, 279 (2004) (Imposing a duty is “an  
10 expression of policy considerations leading to the legal conclusion that a plaintiff is entitled to a  
11 defendant’s protection.”) (quoting *Ludwig v. City of San Diego*, 65 Cal. App. 4th 1105, 1110  
12 (1998)); accord *Tarasoff v. Regents of Univ. of California*, 551 P.2d 334, 342 (Cal. 1976) (“legal  
13 duties are not discoverable facts of nature, but merely conclusory expressions that, in cases of a  
14 particular type, liability should be imposed for damage done”).

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

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

1 In sum, a “special relationship” can create a duty to act even when one otherwise would not  
2 have such a duty. *Zelig*, 45 P.3d at 1183. Ultimate Software thus can be responsible for its  
3 nonfeasance (its failure to act) if (1) it had a special relationship with a third-party actor and thus  
4 had a duty to control that actor, or (2) it had a special relationship with Mr. Greer and thus owed  
5 him a duty to protect him. *Id.* The plaintiff argues that like any business, Ultimate Software has a  
6 “special relationship” with its customers that creates a duty to warn them of known risks.<sup>54</sup>

7 Courts commonly involve the special-relationship doctrine “in cases involving the  
8 relationship between business proprietors such as [landlords,] shopping centers, restaurants, and  
9 bars, and their tenants, patrons, or invitees.” *McGarry*, 158 Cal. App. 4th at 995 (quoting  
10 *Delgado v. Trax Bar & Grill*, 113 P.3d 1159, 1165 (Cal. 2005)). “A business owner may have an  
11 affirmative duty to ‘control the wrongful acts of third persons which threaten invitees where the  
12 [business owner] has reasonable cause to anticipate such acts and the probability of injury  
13 resulting therefrom.’” *Id.* (citing *Taylor v. Centennial Bowl, Inc.*, 416 P.2d 793 (1966)). “The  
14 doctrine also extends to other types of special relationship[s] . . . including those between common  
15 carriers and passengers, and mental health professionals and their patients.” *Id.* (quoting *Tarasoff*,  
16 551 P.2d at 334). These “special relationships generally involve some kind of dependency or  
17 reliance.” *Olson v. Children’s Home Soc’y*, 204 Cal. App. 3d 1362, 1366 (1988); *see e.g.*,  
18 *Williams v. State of California*, 664 P.2d 137, 139 (Cal. 1983) (a factor supporting a special  
19 relationship is detrimental reliance by a person on another person’s conduct that induced a false  
20 sense of security and worsened the position of the person relying on the conduct).

21 “[T]he use of special relationships to create duties has been largely eclipsed by the more  
22 modern use of balancing policy factors enumerated in *Rowland* [*v. Christian*.]” *McGarry*, 158  
23 Cal. App. 4th at 996 (quoting *Doe I v. City of Murrieta*, 102 Cal. App. 4th 899, 918 (2002))  
24 (citing *Rowland v. Christian*, 443 P.2d 561, 564 (Cal. 1968)). The *Rowland* factors are the  
25 following: “[ (1) ] the foreseeability of harm to the plaintiff, [ (2) ] the degree of certainty that the  
26 plaintiff suffered injury, [ (3) ] the closeness of the connection between the defendant’s conduct and  
27

28 <sup>54</sup> Motion to Dismiss – ECF No. 15 at 26.

1 the injury suffered, [(4)] the moral blame attached to the defendant’s conduct, [(5)] the policy of  
2 preventing future harm, [(6)] the extent of the burden to the defendant and consequences to the  
3 community of imposing a duty to exercise care with resulting liability for breach, and [(7)] the  
4 availability, cost, and prevalence of insurance for the risk involved.” *Id.* at 996–97 (quoting  
5 *Rowland*, 443 P.2d at 564); *see also Hansra v. Superior Court*, 7 Cal App. 4th 630, 646 (1992)  
6 (“whether a special relationship exists giving rise to a duty to protect . . . [involves] consideration  
7 of the same factors underlying any duty of care analysis”).

8 Following remand of the *Internet Brands* case, the district court addressed whether a website  
9 has a “special relationship” with its users that required the website to warn users of known risks on  
10 the website. *See Jane Doe No. 14 v. Internet Brands, Inc.*, No. 2:12-CV-3626-JFW (PJW), ECF  
11 No. 51 (C.D. Cal. Nov. 14, 2016). The court found no special relationship and thus no duty to  
12 warn. *Id.* at 5–6.

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

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

26 Another district court — again on remand from the Ninth Circuit — also concluded that a  
27 website had no duty to warn its users. *Beckman v. Match.com, LLC*, No. 2:13-CV-97 JCM (NJK),  
28 2017 WL 1304288, at \*4 (D. Nev. Mar. 10, 2017). The plaintiff met and dated a man on

1 Match.com and ended their relationship eight days later. *Id.* at \*1. He then sent her threatening  
 2 messages for about four days, and four months later, attacked her viciously. *Id.* She sued  
 3 Match.com for failure to warn her that the website and her attacker were dangerous, basing her  
 4 claim in part on Match.com’s access to data about its users and use of the data to create matches.  
 5 *Id.* at \*1–\*3. Applying Nevada law, which is similar to California law, the court found no special  
 6 relationship between Match.com and the plaintiff. *Id.* at \*3–\*4. The plaintiff was merely a paying  
 7 subscriber, paid the fee, set up her profile, and was matched with the attacker. *Id.* at \*3. The court  
 8 concluded that the website had no special relationship with the plaintiff and thus no duty to warn  
 9 her. *Id.* at \*4.

10 These cases support the conclusion that a website has no “special relationship” with its users.  
 11 Ms. Dyroff nonetheless contends that websites operators such as Ultimate Software are the  
 12 “twenty-first century equivalent of a brick and mortar business. . . like restaurants, bars, . . .  
 13 amusement parks, and all businesses open to the public” and have the same duty that all  
 14 businesses open to the public owe their invitees. The duty “includ[es] ‘tak[ing] affirmative action  
 15 to control the wrongful acts of third persons which threaten invitees where the occupant has  
 16 reasonable cause to anticipate such acts and the probability of injury resulting therefrom.’”<sup>55</sup>

17 If the court followed this approach, it would render all social-network websites potentially  
 18 liable whenever they connect their members by algorithm, merely because the member is a  
 19 member. This makes no sense practically. Imposing a duty at best would result in a weak and  
 20 ineffective general warning to all users. *Internet Brands*, No. 2:12-cv-3626-JFW (PJW), ECF No.  
 21 51 at 6. It also “likely [would] have a ‘chilling effect’ on the [I]nternet by opening the floodgates  
 22 of litigation.” *Id.* at 7 (referencing the briefs in the Ninth Circuit). Also, the court is not convinced  
 23 that a bricks-and-mortar business (such as a bar where people meet more obviously) is a good  
 24 analogue to a social-network website that fosters connections online. For one, allocating risk is (in  
 25 part) about foreseeability of harm and the burdens of allocating risk to the defendant or the  
 26

27 \_\_\_\_\_  
 28 <sup>55</sup> Opposition to Motion to Dismiss – ECF No. 15 at 24–26 (quoting *Taylor v. Centennial Bowl, Inc.*,  
 416 P.2d 793, 797 (Cal. 1996)).



1 plaintiff. *See Rowland*, 443 P.2d at 561. Risk can be more apparent in the real world than in the  
2 virtual social-network world.<sup>56</sup> That seems relevant here, when the claim is that a social-network  
3 website ought to perceive risks — through its automatic algorithms and other inputs — about a  
4 drug dealer on its site.

5 Moreover, even if Ultimate Software had superior knowledge about Mr. Margenat-Castro’s  
6 selling fentanyl-laced heroin, that knowledge does not create a special relationship absent  
7 dependency or detrimental reliance by its users, including Mr. Greer. *Internet Brands*, No. 2:12-  
8 cv-3626-JFW (PJW), ECF No. 51 at 6 (“it may have been foreseeable that [the two men] would  
9 strike again”). For example, in *Conti v. Watchtower Bible & Tract Society of New York, Inc.*, the  
10 California Court of Appeal held that a religious organization had no special relationship with its  
11 congregation and thus had no duty to warn them — despite its knowledge of the high risk of  
12 recidivism — that a fellow member was a child molester. *Id.* (citing *Conti*, 235 Cal. App. 4th 1214  
13 (2015), as the case with the most analogous facts). In *Olson*, the California Court of Appeal held  
14 that there was no ongoing “special relationship” between an adoption agency and a birth mother  
15 who gave up her son for adoption that required the agency to notify the birth mother when it  
16 learned that the son tested positive for a serious inherited disease passed from mothers to their  
17 male offspring. *Olson*, 204 Cal. App. 3d at 1366–67. The birth mother later had a second son with  
18 the same affliction. *Id.* By contrast, a duty can arise for a defendant with superior knowledge if  
19 there is dependency or reliance. *See Internet Brands*, No. 2:12-cv-3626-JFW (PJW), ECF No. 51  
20 at 6 n.3 (citing *O’Hara v. Western Seven Trees Corp.*, 75 Cal. App. 3d 798 (1977)). In *O’Hara*,  
21 the landlord had a duty to warn his tenant, who was raped, about the risks because he knew of  
22

---

23 <sup>56</sup> Ms. Dyroff cites *eBay, Inc. v. Bidder’s Edge, Inc.* to support the conclusion that a business’s liability  
24 does not turn on the difference between a bricks-and-mortar business and an Internet business.  
25 Opposition to Motion to Dismiss – ECF No. 15 at 24–25 (citing 100 F. Supp. 2d 1058, 1065 (N.D.  
26 Cal. 2000)). *eBay* does not change the court’s conclusion. In *eBay*, the court granted eBay a  
27 preliminary injunction to prevent a competing auction website from scanning eBay’s website for  
28 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.



1 prior rapes at the apartment complex, knew about the likelihood of a repeat attack because police  
2 gave him composite drawings of the suspect and a description of his modus operandi, failed to  
3 warn his tenant, and assured her that the premises were safe and patrolled at all times by  
4 professional guards). *Id.* (citing *O’Hara*, 75 Cal. App. 3d 798). Here, Ms. Dyroff has not alleged  
5 dependency or reliance.

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

### 8 **2.2 Duty to Warn — Misfeasance (Creation of Risk)**

9 Ms. Dyroff also contends that Ultimate Software created a risk of harm through its website  
10 functionalities and thus owed her son an ordinary duty of care to warn him about Mr. Margenat-  
11 Castro’s trafficking of fentanyl-laced heroin.<sup>57</sup> The court holds that Ultimate Software’s use of the  
12 neutral tools and functionalities on its website did not create a risk of harm that imposes an  
13 ordinary duty of care. *See Lugtu*, 28 P.3d at 256–57 (negligence standard for misfeasance). A  
14 contrary holding would impose liability on a social-network website for using the ordinary tools of  
15 recommendations and alerts. The result does not change merely because Experience Project  
16 permitted anonymous users.

### 17 **2.3 Assumption of Risk**

18 The last issue is whether the assumption-of-risk doctrine bars Mr. Greer’s failure-to-warn  
19 claim. Because the court holds that there is no duty to warn, it does not reach the issue. If it were  
20 to reach the issue, it would likely hold that the doctrine operates as a complete bar to his claim  
21 because Mr. Greer — who initiated the contact with Mr. Margenat-Castro by his posts on  
22 Experience Project and then bought drugs from him — assumed the obviously dangerous risk of  
23 buying drugs from an anonymous Internet drug dealer. *See, e.g., Souza v. Squaw Valley Ski Corp.*,  
24 138 Cal. App. 4th 262, 266–67 (2006).

25 \* \* \*

26  
27  
28 <sup>57</sup> Opposition to Motion to Dismiss – ECF No. 15 at 26.

**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: November 26, 2017



---

LAUREL BEELER  
United States Magistrate Judge

United States District Court  
Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28