Filed 3/15/24

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

STEVE WOZNIAK et al., Plaintiffs and Appellants, v. YOUTUBE, LLC et al., Defendants and Respondents.	H050042 (Santa Clara County Super. Ct. No. 20CV370338)

This lawsuit stems from a common cryptocurrency scam perpetrated on YouTube: popular channels are hijacked to show fake videos depicting a tech celebrity hosting a live event, during which anyone who sends cryptocurrency to a specified account will receive twice as much in return. Users who send their cryptocurrency in response actually receive nothing in return.

Plaintiffs are Steve Wozniak—whose YouTube channel was among those hijacked—and 17 individuals who fell victim to the scam and lost varying amounts of cryptocurrency. They sued YouTube and Google (defendants), asserting nine causes of action alleging that defendants have been knowingly hosting, promoting, and profiting from the scam for years.

The trial court sustained defendants' demurrer on the ground that plaintiffs' claims are barred by the Communications Decency Act of 1996, 47 U.S.C. § 230 (section 230), which generally provides immunity to interactive computer services that a plaintiff seeks to treat as a publisher or speaker of information provided by another content provider.

On appeal, plaintiffs argue their claims are not subject to section 230 immunity because they do not seek to treat defendants as a publisher or speaker of third-party content, but instead seek to hold them liable for engaging in actions they knew would further criminal activity, thereby materially contributing to its illegality.

We hold that most of plaintiffs' claims seek to treat defendants as a publisher or speaker of third-party content and are therefore precluded by section 230. However, we also conclude that one of plaintiffs' claims—that defendants created their own content and materially contributed to the unlawfulness of the scam by providing verification badges to hijacked YouTube channels—includes allegations which potentially could fall outside the scope of section 230 immunity. As currently pleaded, though, we are unable to conclude that those allegations save any of plaintiffs' causes of action.

Nevertheless, because there is a reasonable possibility plaintiffs could cure the defects, we also conclude the trial court abused its discretion in not granting leave to amend the claims related to verification badges. Accordingly, we reverse and remand for further proceedings.

I. FACTUAL AND PROCEDURAL BACKGROUND[1]

A. YouTube cryptocurrency scams

YouTube, LLC (YouTube) is a video-sharing service that enables its users to view, post, and comment on video content hosted on its platform.[2] Users can create their own YouTube channels, thereby making it easy for other users to find a creator's content in one place and be notified when new content is uploaded. The most popular YouTube channels have millions of subscribers.

---

[1] "We derive our facts from those properly pleaded in the complaint and matters properly judicially noticed. [Citations.] We take as true properly pleaded material facts alleged in the pleadings, disregarding contentions, deductions, and conclusions of fact or law. [Citation.]" (*County of Santa Clara v. Superior Court* (2023) 87 Cal.App.5th 347, 355, fn. 2.)

[2] YouTube is a wholly owned and controlled subsidiary of defendant Google, LLC (Google).

User-personalized video recommendations appear when a user first opens the YouTube website or mobile app, and then automatically play after a video ends. YouTube utilizes an algorithm that recommends videos to users based on their personal information and data that YouTube and Google have collected, including clicks, watch time, likes and dislikes, comments, and upload frequency.

According to plaintiffs, YouTube's lax security practices over the years have led to a steady stream of security breaches through which popular YouTube channels are hijacked and taken over by criminals who then use the channels to perpetrate a scam that has defrauded YouTube users of millions of dollars. YouTube has not only knowingly allowed the security breaches and scams, it has also affirmatively promoted and profited from them.

The scam generally operates as follows. First, scammers will breach YouTube's security to unlawfully gain access to verified and popular YouTube channels with tens or hundreds of thousands of subscribers. The scammers then transfer ownership or control of the channel to themselves or a co-conspirator, rename the channel to impersonate tech celebrities or companies, and delete the channel's pre-existing content.

Next, they upload and play scam videos they have created using pre-existing images and videos of famous tech entrepreneurs such as plaintiff Wozniak, Bill Gates or Elon Musk speaking at a cryptocurrency or technology conference, which is intended to deceive YouTube users into believing that the celebrity is hosting a live "bitcoin giveaway" event.[3] Plaintiffs allege that Wozniak, who co-founded Apple Computer in the 1970s, is a "Silicon Valley icon," who has "engaged in many entrepreneurial and philanthropic ventures" and is a "widely known, recognized, and beloved public figure."

---

[3] "Bitcoin is among the world's most well-known digital currencies…." (*Archer v. Coinbase, Inc.* (2020) 53 Cal.App.5th 266, 269.) "A digital currency (also known as 'cryptocurrency') is a type of currency maintained by a decentralized network of participants' computers, rather than a centralized government or organization." (*Ibid*.)

The scam video is surrounded with images and text stating that, for a limited time, anyone who sends bitcoin to a specified account, via a QR code included in the video, will receive twice as much in return. The images and text often include trademarks, such as the Apple logo, and a link to a fraudulent web address that incorporates the particular tech entrepreneur's name. However, after the users transfer their cryptocurrency in an irreversible transaction, they receive nothing in return and the scam is complete.

The scam has existed on YouTube since at least October 2018 and has been replicated many times in substantially the same form. In the process, millions of people have viewed the scam videos, resulting in the loss of millions of dollars of bitcoin and other cryptocurrencies. Specific to this lawsuit, unnamed third parties have perpetrated the scam since at least May 8, 2020, using Wozniak's name and likeness and thereby stealing hundreds of thousands of dollars worth of bitcoin and similar cryptocurrencies from the 17 other named plaintiffs. The scam has continued through the date plaintiffs filed the initial complaint in this action.

According to plaintiffs, defendants have known about the scam, yet have allowed it to continue. In many instances, YouTube knew specific channels had been hijacked but failed to remove or suspend the pre-existing verification badges appearing on those channels. In at least one instance, YouTube issued a verification badge to a channel while it was perpetrating the scam. YouTube has allowed the scam to continue, despite its own stated policies that it does not allow scams or other deceptive practices that take advantage of the YouTube community.

Defendants have both the human and technological capabilities to implement reasonable security measures that would prevent hijacking of popular channels and quickly detect and remove scam videos. Despite having the means to stop or limit the proliferation of the scam, defendants have declined to do so.

According to plaintiffs, beyond merely allowing it to continue, defendants have actively promoted and profited from the scam. For instance, YouTube has promoted the

scam videos in plaintiffs' and other users' home page video recommendations, in their "up-next" videos which often begin playing automatically upon the conclusion of the previous video, and in the list of recommended videos shown while one video is playing. YouTube's algorithm targets the scam videos directly at plaintiffs because the personal information and data that defendants have collected about them—such as clicks, watch time, likes and dislikes, comments, upload frequency, emails sent and received, saved photos and videos, documents and spreadsheets created, YouTube video comments, and other behavior through their apps, browsers, and devices—indicated they were interested in cryptocurrency.

YouTube also issues verification badges to certify to its users that a verified channel has been vetted and is trustworthy. According to plaintiffs, in issuing a verification badge, YouTube is communicating that an account is "the official channel of a creator, artist, company or public figure" and therefore can be trusted. YouTube has maintained verification badges on channels it knew had been hijacked.

Plaintiffs allege YouTube has also negligently designed its video metrics and other public-facing features of its platform to permit the scammers to falsely represent that large numbers of viewers have "liked" and viewed the videos when they have not. The scammers use bots and other tools to falsely inflate the number of likes, views, and those currently watching, to make the videos appear authentic and more legitimate. Similarly, YouTube enables the scammers to falsely represent that an event is live when it is not.

Lastly, defendants sold the scammers paid advertising space that targeted users based on their browsing history and other personal information defendants have collected and analyzed, which indicates an interest in cryptocurrency. According to plaintiffs, despite knowing about the cryptocurrency scams, defendants have continued to sell scammers "all the targeted scam ads that they are willing to buy," and have delivered those ads directly to plaintiffs and other users likely to be interested in the scam video

content. YouTube has continued selling these targeted advertisements to the scammers, notwithstanding its own stated polices that it verifies the identity of its advertisers.

B. Initial complaints and first demurrer

Plaintiffs filed the initial complaint in this action in San Mateo County Superior Court on July 21, 2020, naming YouTube and Google as defendants.[4] The matter was transferred to Santa Clara County Superior Court, which issued an order deeming the case complex and staying all discovery. On February 16, 2021, plaintiffs filed the first amended complaint (FAC). The FAC alleged causes of action for misappropriation of likeness—brought by Wozniak only—fraud and misrepresentation, aiding and abetting fraud, unfair business practices, negligence, negligent failure to warn, and injunctive relief.

Defendants filed a demurrer to the FAC on April 5, 2021. They argued that plaintiffs' claims are precluded by section 230, which was enacted to protect websites against liability for the failure to remove offensive content. According to defendants, plaintiffs were not contending that YouTube actually perpetrated the scam or created any of its content; instead, they sought to hold YouTube liable for not acting more aggressively to monitor, block and remove the material the third parties posted, or for providing neutral tools to its users that the third parties used to perpetrate the scam. Under section 230, they argued, 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—are barred," ' " citing *Murphy v. Twitter* (2021) 60 Cal.App.5th 12, 26 (*Murphy*).

[4] Plaintiffs include Wozniak, and the following individuals who claim to have been harmed by the cryptocurrency scam on YouTube: Alex Naray, James Denitto, Bernardo Garcia, Alexander Geisler, Asa Jacques, Zhenyu Li, Jin Liu, Anthony Martinez, Harivarmah Nagalinggam, Paul Newman, Myrielle Philistin, Dario Lopez Portilla, Eric Restrepo, Raul Moreño Romero, David Schrader, Luke Thomas and Lung Hung Yang. In this opinion, the term "plaintiffs" refers to all 18 plaintiffs; we refer to the non-Wozniak plaintiffs as the "bitcoin plaintiffs" where necessary to distinguish.

They also argued that, even apart from section 230 immunity, plaintiffs had failed to state a viable cause of action. According to defendants, the law does not recognize a theory of secondary liability for misappropriation of likeness and there is no plausible allegation that YouTube itself actually used Wozniak's likeness. In addition, they argued, plaintiffs cannot establish that YouTube owed them a special duty of care because they did not allege YouTube itself engaged in the allegedly unlawful conduct necessary for each claim.

The trial court sustained the demurrer on section 230 immunity grounds but granted plaintiffs leave to amend.

C. Discovery stay

Prior to filing their second amended complaint, plaintiffs moved to lift the discovery stay. They argued that the critical factual dispute in the case is the extent of defendants' involvement in creating and contributing to the scam videos and advertisements driving the scams. According to plaintiffs, they were entitled to obtain critical facts in defendants' sole possession to more fully support their allegations, and "[p]laintiffs' inability to do so in this case has and continues to severely prejudice their ability to have their grievance fairly and fully heard by the Superior Court."

Defendants opposed the motion, arguing that section 230 provides broad immunity that warrants staying discovery. They contended that courts have consistently stayed discovery when defendants have brought a case-dispositive section 230 defense, and that plaintiffs have not cited any authority involving a section 230 case where a discovery stay has been lifted to allow a party "to conduct intrusive discovery in the face of a broad immunity that the court has already held bars the claims at issue."

The trial court denied plaintiffs' motion. It relied on the "significant public interest" in section 230 to protect websites from ultimate liability and from having to fight costly and protracted legal battles, and on the importance of resolving immunity questions at the earliest possible stage in litigation to avoid unnecessary discovery and

other burdens. The court noted that "federal courts routinely stay discovery in cases apparently subject to Section 230 until the complaint is deemed adequate to avoid [section 230] immunity." According to the court, plaintiffs' "vague contentions" that discovery is necessary fail to explain sufficiently "what sort of facts they believe discovery would reveal that would change the section 230 analysis…." The court added that plaintiffs "might be able to do that in the future, but haven't done that yet."

D. Second amended complaint, demurrer, and motion to lift discovery stay

Plaintiffs filed the operative second amended complaint on September 9, 2021 (SAC). The SAC sets forth the allegations summarized above in the factual background, and asserts nine causes of action: (1) misappropriation of likeness, brought by Wozniak only; (2) fraud and misrepresentation; (3) aiding and abetting fraud; (4) unfair business practices; (5) negligence; (6) negligent design; (7) negligent failure to warn; (8) breach of implied contract; and (9) promissory estoppel.

At the same time they filed the SAC, plaintiffs submitted a renewed motion to lift the discovery stay. They restated their previous arguments that they were entitled to discovery on their initial causes of action, and argued they were also entitled to discovery on their new theories of liability because they did not implicate section 230 immunity. According to plaintiffs, those new theories included: (1) negligent security resulting in the regular hijacking of YouTube channels; (2) negligent design of YouTube video metrics, channel information, and security features; (3) wrongful disclosure of plaintiffs' personal information to scammers, including information indicating plaintiffs' interest in cryptocurrency; (4) promissory estoppel arising from defendants' promises about providing excellent security, scam protection, accurate video metrics and channel information, and responsible use of its users' personal information; and (5) negligent failure to warn plaintiffs about each of the foregoing. Plaintiffs contended that section 230 does not apply to those claims because they do not seek to impose liability on

defendants for their conduct as a publisher or speaker, so the discovery stay should be lifted.

Defendants demurred to the SAC as well, presenting the same general arguments set forth in the initial demurrer, including as to the new causes of action. Defendants also opposed the renewed motion to lift the discovery stay on the same grounds.

E. Trial court ruling

The trial court sustained the demurrer to the SAC and denied the renewed motion to lift the discovery stay. It first addressed plaintiffs' allegations, re-stated from the FAC, that defendants had materially contributed to the illegal scam by actively promoting the videos, selling targeted ads, falsely verifying the channels, and providing false and misleading information to promote the videos. The court held that these actions constituted "neutral tools" and, under existing precedent, plaintiffs cannot plead around section 230 immunity by framing such neutral website features as content. "In sum," the court stated, "all of Plaintiffs' claims seek to hold Defendants liable as the publisher of content created by others, and not for Defendants' own content that 'contributes materially to the alleged illegality of' the scams at issue here."

The court then addressed the new facts and theories alleged in the SAC, specifically security- or design-related claims and contract-related causes of action. With respect to the former, the court concluded that the theories of liability still depend on third-party content, without which no liability could exist. With respect to the latter, the court held that, while styled as claims for breach of contract and negligent misrepresentation, in reality they treat defendants as publishers and seek to hold them liable for third-party conduct, thereby coming within the scope of section 230 immunity.

The court did not address defendants' alternative arguments that, independent of section 230, the causes of action failed to state sufficient claims for relief.

The court sustained the demurrer without leave to amend because plaintiffs had not explained how they could amend the SAC to avoid section 230 immunity, and the

court could not discern any such reasonable possibility. The order was entered on January 26, 2022.

A judgment of dismissal (judgment) was entered on May 4, 2022.

Plaintiffs timely appealed.

II. DISCUSSION

Plaintiffs argue on appeal that (1) section 230 does not apply to the conduct alleged in this case, which seeks to hold defendants liable for choosing to engage in actions they knew would further entirely criminal activity, and (2) the trial court abused its discretion in imposing a blanket stay of all discovery and repeatedly refusing to lift the stay.

Defendants argue that (1) plaintiffs' claims seek to impose liability for harm caused by third-party videos hosted on YouTube, which section 230 precludes; (2) even if section 230 does not apply, plaintiffs have still failed to state viable claims because they improperly attempt to impose vicarious liability for harms caused by unrelated third parties; and (3) the trial court properly exercised its discretion in imposing limits on discovery.

We address these arguments in turn below.

A. Section 230 immunity

1. Applicable law and standard of review

"When reviewing a ruling on a demurrer, we examine de novo whether the complaint alleges facts sufficient to state a cause of action." (*Liapes v. Facebook* (2023) 95 Cal.App.5th 910, 919 (*Liapes*), citing *Regents of University of California v. Superior Court* (2013) 220 Cal.App.4th 549, 558 (*Regents*).) " 'We assume the truth of the properly pleaded factual allegations, [and] facts that reasonably can be inferred from those expressly pleaded.' [Citation.] But we do not assume the truth of 'contentions, deductions, or conclusions of law.' " (*Liapes, supra*, at p. 919, quoting *Stearn v. County of San Bernardino* (2009) 170 Cal.App.4th 434, 440.)

"We liberally construe the complaint 'with a view to substantial justice between the parties,' drawing 'all reasonable inferences in favor of the asserted claims.' " (*Liapes, supra,* 95 Cal.App.5th at p. 919, quoting *Regents, supra*, 220 Cal.App.4th at p. 558.) "The plaintiff must demonstrate the court erroneously sustained the demurrer and 'must show the complaint alleges facts sufficient to establish every element of each cause of action.' " (*Liapes, supra*, at p. 919, quoting *Rakestraw v. California Physicians' Service* (2000) 81 Cal.App.4th 39, 43.)

When a demurrer is sustained without leave to amend, "we decide whether there is a reasonable possibility that the defect can be cured by amendment: if it can be, the trial court has abused its discretion and we reverse; if not, there has been no abuse of discretion and we affirm. [Citations.] The burden of proving such reasonable possibility is squarely on the plaintiff." (*Blank v. Kirwan* (1985) 39 Cal.3d 311, 318 (*Blank*).) In the context of a demurrer on section 230 grounds, "when a plaintiff cannot allege enough facts to overcome Section 230 immunity, a plaintiff's claims should be dismissed." (*Dyroff v. Ultimate Software Group, Inc*. (9th Cir. 2019) 934 F.3d 1093, 1097 (*Dyroff*).)[5]

Section 230 " 'immunizes providers of interactive computer services against liability arising from content created by third parties.' " (*Liapes, supra,* 95 Cal.App.5th at p. 928, quoting *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* (9th Cir. 2008) 521 F.3d 1157, 1162, fn. omitted (*Roommates*).) "Congress enacted section 230 'for two basic policy reasons: to promote the free exchange of information and ideas over the internet and to encourage voluntary monitoring for offensive and

[5] Although federal precedents interpreting section 230 are not binding upon this court, "where the decisions of the federal courts on a federal question are ' " 'both numerous and consistent,' " ' we should hesitate to reject their authority [citation]." (*Doe II v. MySpace, Inc.* (2009) 175 Cal.App.4th 561, 571, quoting *Barrett v. Rosenthal* (2006) 40 Cal.4th 33, 58 (*Barrett*); *Etcheverry v. Tri–Ag Service, Inc.* (2000) 22 Cal.4th 316, 320–321 ["While we are not bound by decisions of the lower federal courts, even on federal questions, they are persuasive and entitled to great weight."].)

obscene material.' " (*Hassell v. Bird* (2018) 5 Cal.5th 522, 534 (*Hassell*), quoting *Carafano v. Metrosplash.com, Inc.* (9th Cir. 2003) 339 F.3d 1119, 1122.)

Section 230, subdivision (c)(1) states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Section 230, subdivision (e)(3) provides: "No cause of action may be brought, and no liability may be imposed under any State or local law that is inconsistent with this section."

An "interactive computer service" is defined in the statute as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." (§ 230, subd. (f)(2).) The statute also defines "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." (§ 230, subd. (f)(3).)

Read together, these two provisions " 'protect 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.' " (*Murphy, supra,* 60 Cal.App.5th at p. 24, quoting *Barnes v. Yahoo!, Inc.* (9th Cir. 2009) 570 F.3d 1096, 1100–1101, fn. omitted (*Barnes*).)[6]

The California Supreme Court has explained that these provisions "convey[] an intent to shield Internet intermediaries from the burdens associated with defending against state law claims that treat them as the publisher or speaker of third party content." (*Hassell, supra,* 5 Cal.5th at p. 544; see also *Barrett, supra,* 40 Cal.4th 33, 39 [section 230, subdivisions (c)(1) and (e)(3) "have been widely and consistently interpreted to

[6] The parties agree that YouTube is an interactive computer service—accordingly, our discussion below focuses only on the second and third elements.

confer broad immunity against defamation liability for those who use the Internet to publish information that originated from another source"].)

"Accordingly, section 230 protects an interactive computer service provider's curation of content on its platform from ' " ' claims that would place a computer service provider in a publisher's role. Thus, 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—are barred.' " ' (*Prager University v. Google, LLC* (2022) 85 Cal.App.5th 1022, 1032 (*Prager*), quoting *Barrett, supra*, 40 Cal.4th at p. 43.)

Notwithstanding that broad construction of section 230, "an interactive computer service provider only has immunity if it is *not* also the information content provider — that is, someone 'responsible, in whole or in part, for the creation or development' of the content at issue." (*Liapes, supra,* 95 Cal.App.5th at p. 928, citing § 230, subd. (f)(3), *Roommates, supra,* 521 F.3d at p. 1162.) "Passively displaying content 'created entirely by third parties' renders the operator only a service provider 'with respect to that content.' (*Roommates*, at p. 1162.) '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.' [Citation.] '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.' " (*Liapes, supra,* 95 Cal.App.5th at p. 928.)

A website creates or develops content "by making a material contribution to [its] creation or development." (*Kimzey v. Yelp, Inc.* (9th Cir. 2016) 836 F.3d 1263, 1269 (*Kimzey*).) A "material contribution" does not refer to "merely . . . augmenting the content generally, but to materially contributing to its alleged unlawfulness." (*Roommates, supra*, 521 F.3d at pp. 1167-1168.)

2. Analysis

In their briefs on appeal, plaintiffs group their claims into six general categories, rather than addressing each of the nine causes of action individually. Our discussion below tracks those six categories.

a. Negligent security claim

Plaintiffs characterize their "negligent security claim" as an allegation that defendants "failed to implement reasonable security measures to protect verified and popular YouTube channels from being regularly hijacked and transformed to broadcast the scam videos." Plaintiffs contend this claim does not treat defendants as the publisher or speaker of third-party content, and section 230 does not immunize failures to secure software from intrusion. They argue that the negligent-security claim is "not concerned with whether YouTube engaged in traditional editorial functions immunized by Section 230, such as blocking or removing user content." Instead, they argue, the claim is concerned with the failure to employ reasonable security measures to protect channels from hijacking.

Applying the standards summarized above, we conclude plaintiffs' negligent security claim is subject to section 230 immunity because it seeks to treat defendants as a publisher and speaker of information provided by another information content provider. (*Murphy, supra,* 60 Cal.App.5th at p. 24.) In their briefs, plaintiffs do not identify which causes of action include their "negligent security" claim, and there is no claim in the SAC with that label. Instead, plaintiffs cite various allegations from the SAC which are found within the "negligence" cause of action. We construe this as a concession that the other causes of action do not purport to allege liability for these "security-related" claims, and we limit our analysis here to the negligence cause of action.

In the negligence cause of action, plaintiffs allege, among other things, that: defendants had knowledge of all relevant aspects of the scam before plaintiffs were harmed by it; defendants owed plaintiffs a duty to use reasonable care to prevent harm to

others, including to prevent or mitigate the foreseeable risk that plaintiffs and other users would be victimized by the scam; defendants breached that duty by failing to implement reasonable security protocols to prevent or shut down the scam on their platforms; and, plaintiffs were harmed by those breaches.

Ultimately, this claim seeks to hold YouTube liable for allowing the scam videos to be shown on the hijacked channels. YouTube's actions allowing the scam videos to be shown on hijacked channels amount to a publishing decision not to prevent or alter the videos—that is, " 'deciding whether to exclude material that third parties seek to post online.' " (*Murphy, supra,* 60 Cal.App.5th at p. 24, quoting *Roommates, supra*, 521 F.3d at pp. 1170-1171.) Plaintiffs insist their claim is not concerned with whether YouTube engaged in traditional editorial functions such as blocking or removing user content; instead, they allege defendants failed to implement "common-sense security measures to prevent rampant hijacking and unfettered repurposing of YouTube channels and the resulting harm to users, including Plaintiffs." In other words, they argue their claim is content-neutral because it is not predicated on the harmful content that flowed from the security failures.

Plaintiffs rely solely on a recent case from the northern district of California—*In re Zoom Video Communications Inc. Privacy Litigation* (N.D. Cal. 2021) 525 F.Supp.3d 1017 (*In re Zoom*). In that case, the plaintiffs were Zoom users who alleged that Zoom had made harmful misrepresentations and failed to secure Zoom meetings from intruders known as "Zoombombers." (*Id*. at p. 1023.) The plaintiffs argued that they sought to hold Zoom accountable not for its actions as a content provider, publisher or speaker, but rather for its failure to provide promised security and privacy. (*Id.* at p. 1030.) Zoom moved to dismiss, arguing that section 230 immunized them from all such claims. (*Ibid*.)

The court analyzed section 230's text, legislative history and case law, and explained that the immunity does not apply to claims that are either (1) content neutral, or (2) do not derive from the defendant's status or conduct as a publisher or speaker. (*Id.* at

p. 1032, citing *HomeAway.com v. City of Santa Monica* (9th Cir. 2019) 918 F.3d 676, 680 [section 230, subdivision (c)(1) immunity does not apply to content-neutral liability); *Nunes v. Twitter* (N.D. Cal. 2016) 194 F.Supp.3d 959, 968 [where statute imposes liability regardless of content, section 230, subdivision (c)(1) immunity does not apply]; *Barnes, supra,* 570 F.3d at p. 1107 [section 230, subdivision (c)(1) did not preclude plaintiff's contract-based liability claims, where contract generated legal duty distinct from Yahoo's status as publisher].)

Under that framework, the court held that the bulk of the plaintiffs' claims were immunized by section 230, because they challenged the harmfulness of specific content provided by the third party Zoombombers and alleged Zoom should have done more to moderate or block that content. (*In re Zoom*, *supra,* 525 F.Supp.3d at p. 1035.) However, the plaintiffs' contract-based claims were not subject to section 230 immunity because they did not derive from Zoom's status or conduct as a publisher or speaker. (*Ibid*.) The court also denied the motion to dismiss the plaintiffs' claims "to the extent they are content-neutral." (*Ibid*.)

We agree with the general proposition described in *Zoom* that section 230 immunity may not apply when a plaintiff alleges harm resulting solely from a security failure or statutory violation, *independent of* any harmful third-party content resulting from the violation. (*In re Zoom, supra,* 525 F.Supp.3d at p. 1032.) However, that is not what plaintiffs alleged here. As we have explained, the negligence cause of action is predicated on YouTube allowing *the scam videos* to be shown on the hijacked channels.

Plaintiffs argue that "[w]hile the content of the scam videos were [sic] themselves also undoubtedly harmful to Plaintiffs, that is separate and distinct from the harm caused by Defendants in failing to remedy known security flaws that Defendants knew criminals were actively exploiting to harm YouTube's users." In other words, plaintiffs seek to characterize their claim as alleging both that (1) the security failure itself caused harm, and (2) the resulting bitcoin scam caused further independent harm.

The allegations in the SAC do not support that characterization, though. Plaintiffs have not alleged that the mere hijacking of Wozniak's and other users' channels, without more, caused them harm. Nor have they alleged that defendants owed them a duty to prevent the hijacking of Wozniak's or other users' channels, regardless of whether any harmful content follows.

The negligence cause of action does include an allegation that defendants owed plaintiffs a duty to take reasonable steps "to design, maintain, implement, monitor, test, and comply with reliable security systems, protocols, and practices to ensure that its website, including YOUTUBE channels, were adequately secured from unauthorized access." Yet, even liberally construing the SAC, we do not read that as an allegation that defendants owed plaintiffs such a duty independent of any resulting harmful content. At bottom, the negligence cause of action and the SAC as a whole demonstrate that plaintiffs' security-based claim is predicated on the harmful content of the scam videos, without which there would likely be no lawsuit. (See, e.g., *Murphy, supra*, 60 Cal.App.5th at p. 30, fn. 6 [gravamen of each cause of action "concern[ed] Twitter's editorial decisions not to publish content—as reflected by the fact that [plaintiff] alleges no specific injury from the alleged notice and retroactivity violations but complains instead of the harm caused by Twitter's ban on her and others' free speech rights"].)

Lastly, we recognize that the individual plaintiffs in this action do not make identical allegations. For instance, only the bitcoin plaintiffs allege they were scammed into transferring their cryptocurrency, and only Wozniak alleges that his YouTube channel was hijacked, thereby causing reputational damage. However, the allegations in the negligence cause of action do not distinguish between Wozniak and the bitcoin plaintiffs. Nor have plaintiffs argued in their briefs that any individual plaintiffs made different allegations in support of their negligent security claim.

b. Negligent design claim

Plaintiffs' characterization of their negligent design claim is similar to that of their negligent security claim. They argue that the duty defendants violated springs from their distinct capacity as product designers rather than as publishers or speakers, and that plaintiffs allege design flaws that do not derive from the content of third-party videos or posts. For the same reasons set forth above regarding the negligent-security claim, we conclude this claim seeks to treat defendants as a publisher and speaker of information provided by another information content provider. (*Murphy, supra,* 60 Cal.App.5th at p. 24.)

In support of their arguments, plaintiffs cite allegations in their negligence and negligent design causes of action. The negligent design claim makes similar allegations as the negligence claim. For instance, it alleges that YouTube negligently designed its security protocols and video metrics such as likes, dislikes, views, "currently watching" count, livestream indicator, and verification badges. As a result, YouTube's platform is "easily exploitable by bad actors" and "allow[s] scammers free reign to modify hijacked channels to perpetrate the scam—all while assuring its users these issues do not exist." They further allege that those video and channel metrics "did not perform as safely as an ordinary consumer would have expected them to perform when used in an intended or reasonably foreseeable way, such as occurred when Plaintiffs used YOUTUBE to watch videos and were scammed out of cryptocurrency due in significant part to the false and misleading video metrics and other information displayed about the scam videos, and which were a significant factor and cause in Plaintiffs believing the scam videos were legitimate and in transferring their cryptocurrency to the scammers."

Ultimately, this claim seeks to hold YouTube liable for allowing the scam videos to be shown on the hijacked channels and is predicated on that third-party content. YouTube's actions amount to a publishing decision not to prevent or alter the videos—that is, " 'deciding whether to exclude material that third parties seek to post online.' "

(*Murphy, supra,* 60 Cal.App.5th at p. 24, quoting *Roommates, supra*, 521 F.3d at pp. 1170-1171.)

Plaintiffs rely on *Lemmon v. Snap, Inc.* (9th Cir. 2021) 995 F.3d 1085 (*Lemmon*). In that case, a 20-year-old man and two 17-year-old boys died after driving their car over 100 miles per hour and crashing into a tree. (*Id*. at p. 1089.) Shortly before the crash, one of the boys had opened the Snapchat application on his smartphone to document how fast they were driving. (*Ibid*.) The boys' parents sued Snap, the social media provider that owns the Snapchat application, alleging it encouraged their sons to drive at dangerous speed and thus caused their death through the negligent design of its application. (*Id.* at p. 1090-1091.) Specifically, they alleged that the application uses a "speed filter"—which allows users to record and share their real-life speed—and a reward system with trophies and social recognitions, combining to create an incentive for users to reach 100 miles per hour and document it on the application. (*Id*. at p. 1089.)

The court held that the negligent design claim was not barred by section 230. The parents' claim rested on the premise that manufacturers have a duty to exercise due care in supplying products that do not present an unreasonable risk of injury or harm to the public. (*Lemmon, supra*, 995 F.3d at p. 1091-1092.) As the court explained, "[t]he duty underlying such a claim differs markedly from the duties of publishers as defined in the CDA. Manufacturers have a specific duty to refrain from designing a product that poses an unreasonable risk of injury or harm to consumers. [Citation.] Meanwhile, entities acting solely as publishers—*i.e.*, those that 'review[ ] material submitted for publication, perhaps edit[ ] it for style or technical fluency, and then decide[ ] whether to publish it,' [citation]—generally have no similar duty." (*Id*. at p. 1092.) The duty that Snap allegedly violated " 'springs from' its distinct capacity as a product designer," as "evidenced by the fact that Snap could have satisfied its 'alleged obligation'… without altering the content that Snapchat's users generate." (*Id*. at p. 1092, quoting *Barnes, supra*, 570 F.3d at p. 1107.)

We find the case distinct for the same general reasons set forth above with respect to *In re Zoom*. While the negligent design claim in *Snap* was not predicated on any third-party content—indeed, the alleged harm flowed directly and solely from the negligent design and occurred without any third-party content—the same is not true here. Instead, the negligent design claim and the SAC as a whole are predicated on the scam videos, without which there would likely be no lawsuit. While a plaintiff *may* avoid application of section 230 immunity by alleging a negligent design claim that is independent of third-party content, that is not what plaintiffs alleged in the SAC here.

c. Negligent failure to warn claim

Plaintiffs argue that their negligent failure to warn cause of action is not immunized by section 230. According to plaintiffs, section 230 does not apply because (1) they allege defendants knew about the scam without having to monitor any third-party content, and (2) there is no exception to the duty of care defendants owed plaintiffs.

With respect to the first of those arguments, plaintiffs rely on *Doe v. Internet Brands, Inc.* (9th Cir. 2016) 824 F.3d 846. In that case, two men used a networking website for models to lure women to fake photo shoots, where they drugged and raped them. (*Id*. at pp. 848-849.) The plaintiff, one of the victimized women, sued the website for negligent failure to warn, alleging it knew of the ongoing scheme but breached its duty to warn her and other users. (*Ibid*.) The Ninth Circuit held that section 230 did not bar the plaintiff's claim because she did not seek to hold the defendant liable as a publisher or speaker of any third-party content. (*Id.* at p. 851.) Instead, she sought to hold it liable for failing to warn about information it had obtained from an outside source about the scheme. (*Ibid*.)

Again, we find the case inapposite. Here, plaintiffs' claim is predicated on the third-party content, of which they assert defendants had a duty to warn. Plaintiffs thus seek to impose liability on defendants resulting from the third-party information they publish on their platform. In *Internet Brands*, by contrast, the alleged duty to warn

existed independent of any third-party content on the defendant's platform. The plaintiff there alleged a duty to warn of the possibility of being drugged and raped at a fake photo shoot—in so doing, she was not treating the defendant as a publisher or speaker of third-party information.

With respect to plaintiffs' second argument, they contend defendants owed them a tort duty to warn pursuant to the basic principle in Civil Code section 1714, subdivision (a) that "[e]veryone is responsible, not only for the result of his or her willful acts, but also for an injury occasioned to another by his or her want of ordinary care or skill in the management of his or her property or person," and that no exception exists.

However, section 230 is an exception. (*Prager, supra*, 85 Cal.App.5th at p. 1043 ["Section 230(c)(1) and (e)(3) reflect the unambiguous exercise of Congress's constitutional power to preempt state laws"].) It provides immunity from certain causes of action that seek to treat defendants as a publisher or speaker of information provided by another information content provider. (*Murphy, supra,* 60 Cal.App.5th at p. 24.) Plaintiffs' argument would allow essentially every state cause of action otherwise immunized by section 230 to be pleaded as a failure to warn of such information published by a defendant. That construction of the law runs counter to the authority we have summarized above.

d. Claims based on knowingly selling and delivering scam ads and scam video recommendations to vulnerable users

Plaintiffs argue section 230 does not immunize from claims that defendants (1) knowingly sold and delivered scam advertisements, or (2) recommended scam videos to vulnerable users. Plaintiffs' theory is that defendants are "knowingly selling criminals the ads necessary to fuel their criminal activity, and the ads are being purchased with the proceeds of their criminal activity," constituting "financial entanglement" that falls outside the scope of section 230 immunity. In addition, they are "recommending scam

videos or other activity involving algorithms to knowingly help criminals target vulnerable users."

Plaintiffs characterize these as independent theories of liability "underlying most of [their] claims." They specifically cite allegations in the SAC found in the negligence, negligent failure to warn, and breach of implied contract causes of action.

First, we address plaintiffs' arguments regarding the sale of advertisements. As with their previous claims, this, too, is ultimately predicated on the third-party content of the scam videos. Plaintiffs do not object to the mere act of defendants selling advertisements to third parties. Instead, they object to the content of the advertisements themselves, which promote the scam. For instance, in the negligence cause of action, they allege that defendants breached their duties by, among other things, "selling ads for, and otherwise promoting, materially contributing to, and profiting from the scam." There is no allegation that selling advertisements, by itself and independent of their content, constituted the breach. Nor is there any allegation that defendants themselves created the advertisements or any of their content. Instead, the claims treat defendants as the publisher of those advertisements. (*Murphy, supra,* 60 Cal.App.5th at p. 24.)

Plaintiffs argue that defendants' "financial entanglement" and "revenue sharing" with the third-party criminals takes them outside the scope of section 230 immunity. They rely on a recent case from the Ninth Circuit Court of Appeals—*Gonzalez v. Google, LLC* (9th Cir. 2021) 2 F.4th 871 (*Gonzalez*), *reversed on other grounds by Twitter, Inc. v. Taamneh* (2023) 598 U.S. 471. In *Gonzalez*, the plaintiffs were the families of victims of attacks by the terror group ISIS. They sued Google, Twitter and Facebook, alleging that the social media platforms allowed ISIS to post videos and other content to communicate their message, radicalize new recruits, and further its mission. (*Gonzalez, supra,* 2 F.4th at p. 880.) They also claimed that Google placed paid advertisements in proximity to ISIS-created content and shared the resulting ad revenue with ISIS. (*Ibid.*) Accordingly, they alleged, the defendants were directly liable for committing acts of international

terrorism pursuant to the Anti-Terrorism Act, 18 U.S.C. § 2333, and secondarily liable for conspiring with, and aiding and abetting, acts of international terrorism. (*Ibid*.)

The Ninth Circuit held that the plaintiffs' revenue-sharing theory was distinct from the other theories of liability, as it was "not directed to the publication of third-party information," but instead was "premised on Google providing ISIS with material support by giving ISIS money." (*Gonzalez, supra,* 2 F.4th at 898.) The court explained that the revenue-sharing theory did not depend on "the particular content ISIS places on YouTube; this theory is solely directed to Google's unlawful payments of money to ISIS." (*Ibid.*) For that reason, section 230 immunity did not apply to the revenue-sharing claims. (*Id.* at pp. 898-99.)

We find the case distinct. Here, plaintiffs do not allege that defendants gave money directly to the third-party scammers. There is no allegation of wrongdoing that is not dependent on the content of the third-party information. While plaintiffs allege that defendants knowingly profited from the advertisements and the associated criminal scheme, *Gonzalez* did not hold that profiting from third-party advertisements is beyond the scope of section 230 immunity. Instead, it distinguished between activity that depended on the particular content placed on YouTube, and activity that did not, such as directly providing material support to ISIS by giving them money.

Plaintiffs' second theory is that section 230 does not immunize from claims that defendants are "recommending scam videos or other activity involving algorithms to knowingly help criminals target vulnerable users." They argue courts have interpreted *Gonzalez* as holding that the products of purportedly neutral website algorithms—such as targeted ads and recommendations—are outside the bounds of Section 230 "if the site owner is alleged to have knowingly assisted wrongdoers who harness those algorithms to inflict harm." They rely on a case from the southern district of New York—*National Coalition on Black Civic Participation v. Wohl* (S.D.N.Y., Sept. 17, 2021, 20 Civ. 8668 (VM)) 2021 U.S. Dist. Lexis 177589* (*Wohl*). In *Wohl*, the defendants allegedly sent

robocalls containing false information intended to prevent recipients from voting, in violation of the Voting Rights Act of 1965 and Ku Klux Klan Act of 1870. The court held that section 230 immunity did not apply because the defendants had acted as more than a passive publisher or neutral intermediary. Rather than merely transmitting robocall messages, the defendants allegedly had discussed the content or purpose of the messages, maintained a database of phone numbers that could be targeted for a robocall campaign, and directed the messages to specific communities and zip codes selected by certain defendants, "to maximize the threatening effects the robocall would have on Black voters in New York and other large metropolitan areas." (*Id*. at p. 8.)

The court acknowledged that "the use of neutral algorithms does not constitute content development." (*Wohl, supra,* 2021 U.S. Dist. Lexis 177589* at p. 9.) However, it held that the claims at issue were not based on the mere provision or use of content-neutral tools in a neutral manner. (*Ibid*.) Instead, they alleged the defendants actively and specifically aided the illegal behavior, including by curating a list of target zip codes. (*Ibid*.)

We do not find the case analogous. Here, plaintiffs have not alleged that defendants undertook any similar acts to actively and specifically aid the illegal behavior. Instead, they allege only that YouTube's neutral algorithm results in recommending the scam videos to certain targeted users. For instance, the SAC alleges that "YouTube's state-of-the-art algorithm tailors its recommended videos to its users based on a variety of personal information and data that YOUTUBE and GOOGLE collect about their users, including 'clicks, watch time, likes/dislikes, comments, freshness, and upload frequency.' " There is no allegation that YouTube has done anything more than develop and use a content-neutral algorithm.

Courts have consistently held that such neutral tools do not take an interactive computer service outside the scope of section 230 immunity. In *Dyroff*, for instance, the plaintiff was the family of a man who had died after using fentanyl-laced heroin, which

he had acquired following communications on defendant's online messaging board. (*Dyroff, supra,* 934 F.3d at p. 1094.) The plaintiff contended the messaging board created content because it "used features and functions, including algorithms, to analyze user posts ... and recommend other user groups." (*Id*. at p. 1098.) The Ninth Circuit rejected the argument, holding that "[t]hese functions—recommendations and notifications—[were] tools meant to facilitate the communication and content of others," and were "not content in and of themselves." (*Ibid*.)

The online message board employed neutral tools similar to the ones challenged by plaintiffs here, and there is no allegation that the algorithms treat the scam content differently than any other third-party content. (*Ibid*.; see also, *Gonzalez, supra*, 2 F.4th at p. 896 ["a website's use of content-neutral algorithms, without more, does not expose it to liability for content posted by a third-party"]; *Roommates, supra,* 521 F.3d at p. 1171 [website not transformed into content creator by virtue of supplying neutral tools that deliver content in response to user inputs]; *cf. Liapes, supra,* 95 Cal.App.5th at p. 929 [Facebook's tools were not neutral—rather than merely proliferate and disseminate content as a publisher, they created, shaped, and developed content by requiring users to provide information used to contribute to discriminatory unlawfulness].)

e. Claims based on wrongful disclosure and misuse of plaintiffs' personal information

Plaintiffs argue that defendants failed to take reasonable measures to protect their personal information from being disclosed to and exploited by scammers. In support of their arguments, plaintiffs cite allegations in their negligence, unfair business practices, breach of implied contract, and promissory estoppel causes of action.

With respect to their breach of implied contract, negligence and unfair business practices causes of action, plaintiffs argue only that, "for reasons similar to those above," they do not seek to hold defendants liable as the publisher or speaker of third-party content, but rather "for their failure to take reasonable measures to ensure they are not

selling targeted scam ads and making recommendations that weaponize Plaintiffs' [personal information] against them." For support, they rely again on *In re Zoom*.

For the same reasons set forth above in the sections discussing plaintiffs' negligence-based claims, we conclude these claims also seek to treat defendants as a publisher and speaker of information provided by another information content provider because they are ultimately predicated on YouTube allowing the scam videos to be shown on the hijacked channels. (*Murphy, supra,* 60 Cal.App.5th at p. 24.)[7]

With respect to their promissory estoppel cause of action, plaintiffs argue that it is based on defendants' "public and widely publicized promises about providing excellent security, protecting against scams, ensuring the accuracy of video metrics and other video and channel information, and using Plaintiffs' personal non-public information and data in a responsible way." According to plaintiffs, their "quasi-contractual claims are based on breaches of duties and promises that have nothing to do with content moderation, such as implied duties and promises to protect Plaintiffs from known security flaws and to protect Plaintiffs' [personal information] from misuse and wrongful disclosure."

Plaintiffs rely chiefly on the Ninth Circuit Court of Appeals' decision in *Barnes* for support. In that case, the plaintiff sued Yahoo after her ex-boyfriend posted unauthorized false profiles of her on its website. (*Barnes, supra*, 570 F.3d at pp. 1098–1099.) In response to her demand that Yahoo remove the profiles, Yahoo's director of communications called her and told her he would " 'personally walk the statements over to the division responsible for stopping unauthorized profiles and they would take care of

---

[7] Plaintiffs cite to the allegations in their breach of implied contract cause of action, but offer no argument in support beyond their reference to "reasons similar to those above." To the extent their argument regarding that cause of action is any different than for their negligence and UCL causes of action, they have failed to support it with reasoned argument and we consider it forfeited. (*Badie v. Bank of America* (1998) 67 Cal.App.4th 779, 784-785 ["When an appellant fails to raise a point, or asserts it but fails to support it with reasoned argument and citations to authority, we treat the point as waived"].)

it.' " (*Id.* at pp. 1098–1099.) After Yahoo still failed to remove the content, Barnes sued, alleging negligence and promissory estoppel. (*Id.*)

The Ninth Circuit drew a distinction between the two types of claims. The negligence claim was barred by section 230 because "the duty that Barnes claims Yahoo violated derives from Yahoo's conduct as a publisher—the steps it allegedly took, but later supposedly abandoned, to de-publish the offensive profiles." (*Barnes, supra*, 570 F.3d at p. 1103.) By contrast, the promissory estoppel claim was not barred because "the duty the defendant allegedly violated springs from a contract—an enforceable promise—not from any non-contractual conduct or capacity of the defendant. [Citation.] Barnes does not seek to hold Yahoo liable as a publisher or speaker of third-party content, but rather as the counter-party to a contract, as a promisor who has breached." (*Id.* at p. 1107.)

Several courts have recently considered the extent to which section 230 bars certain contract-based claims. In *Murphy*, the First District Court of Appeal noted that *Barnes* "never suggested… that *all* contract or promissory estoppel claims survive CDA immunity." (*Murphy, supra,* 60 Cal.App.5th at p. 29.) Instead, *Barnes* had explained that, "as a matter of contract law, the promise must 'be as clear and well defined as a promise that could serve as an offer, or that otherwise might be sufficient to give rise to a traditional contract supported by consideration," and that "a general monitoring policy ... does not suffice for contract liability.' " (*Ibid*., quoting *Barnes*, *supra*, 570 F.3d at p. 1108.) For that reason, the court held that the plaintiff's allegations at issue—that Twitter " 'enforced its Hateful Conduct Policy in a discriminatory and targeted manner' " by removing her tweets and suspending her account—amounted to attacks on Twitter's "interpretation and enforcement of its own general policies rather than breach of a specific promise." (*Murphy, supra,* 60 Cal.App.5th at app. 29-30.)

Similarly, in *Prager*, a different panel of this court acknowledged that section 230 does not necessarily foreclose contractual claims where the defendant "has agreed to limit

its exercise of editorial discretion according to bargained-for terms and conditions." (*Prager, supra,* 85 Cal.App.5th at p. 1035, citing *Murphy, supra*, 60 Cal.App.5th at pp. 28-30.) Nevertheless, the court rejected the plaintiff's various theories of liability that were predicated on the defendants' terms of service, finding each of them deficient "as a matter of either law or pleading." (*Ibid*.)

Defendants' alleged promises here are closer to those in *Murphy*— more akin to general policies or statements—than those in *Barnes*—personalized and constituting a clear, well-defined offer. As noted above, plaintiffs rely on defendants' "public and widely publicized promises." For instance, they cite allegations that Google states on its website: "When people use our products, they trust us with their information, and it's our job to do right by them. This means always being thoughtful about what data we use, how we use it, and how we protect it."

Similarly, they allege that Google states it uses "the world's most advanced security," and "[t]o keep every Google product and service [which includes youtube.com] secure for our users, we engineer and employ one of the most advanced security infrastructures in the world. This means constantly strengthening our built-in security technologies to detect and protect against evolving online threats, before they ever reach our users."

We view these statements as general policies made by defendants in their capacity as publisher, rather than as specific promises. (*Murphy, supra,* 60 Cal.App.5th at app. 29-30.). As such, plaintiffs' claim for promissory estoppel does not survive section 230 immunity.

f. Claims based on defendants' creation or development of information materially contributing to scam ads and videos

Plaintiffs argue defendants were also active content providers that materially contributed to the alleged illegality of the third-party conduct and therefore fall outside the scope of section 230 immunity. Specifically, they argue that, with respect to the

scam, defendants are information content providers under section 230 because they materially contributed to the scam's illegality by creating scam videos and paid advertising; falsely representing that the scam videos were "live" and that large numbers of users were watching or had "liked" the videos; recommending videos and selling advertisements to lead vulnerable users directly to the scam; and falsely displaying "verification badges," thereby communicating that the scam videos represented the real individual or entity it claimed to be "and therefore can be trusted."

As summarized above, "an interactive computer service provider only has immunity if it is *not* also the information content provider — that is, someone 'responsible, in whole or in part, for the creation or development' of the content at issue." (*Liapes, supra,* 95 Cal.App.5th at p. 928.) A website may qualify as an information content provider and lose immunity under section 230 "by making a material contribution to creation or development" of illegal content. (*Kimzey, supra,* 836 F.3d at p. 1269.) A "material contribution" to illegal content refers to "materially contributing to its alleged unlawfulness." (*Roommates, supra*, 521 F.3d at pp. 1167-1168.)

We address plaintiffs' arguments in turn. First, plaintiffs argue on appeal that defendants are information content providers with respect to the scam because they created scam videos and paid advertisements. While such behavior theoretically could make defendants information content providers under section 230, the SAC does not actually allege that *defendants* created scam videos or advertisements. Instead, it alleges that the third-party scammers created the videos and the advertisements, and defendants allowed them to be published on their platforms: "Defendants materially contributed to them by promoting the videos to a specific audience identified through its algorithm, by selling targeted ads driving traffic to the videos, by falsely verifying YOUTUBE channels that carry the videos…."

Second, the SAC similarly does not allege that *defendants* falsely represented that the scam videos were live and that large numbers of users were watching and liked the

videos. Instead, it alleges that defendants "negligently designed video metrics and other public-facing features of its platform that *permit the scammers to falsely represent* that the scam videos are 'live' when they are not, that large numbers of users who are 'currently watching' live scam videos when they are not, that a large number of users have 'viewed' the videos when they have not, that large numbers of users have 'liked' the videos when they have not, and other similarly false or misleading statements of fact that cause the scam videos and promotions to appear authentic." (Emphasis added.) In other words, plaintiffs allege that the scammers created that information, not defendants.

Third, defendants' recommendation of videos and sale of advertisements does not make them information content providers because those recommendations did not materially contribute to the illegality of the content underlying the scam. A "material contribution" does not merely refer to "augmenting the content generally, but to materially contributing *to its alleged unlawfulness*." (*Roommates*, *supra,* 521 F.3d at pp. 1167–68 (emphasis added). "This test 'draw[s] the line at the "crucial distinction between, on the one hand, taking actions" to display 'actionable content and, on the other hand, responsibility for what makes the displayed content [itself] illegal or actionable.' " (*Kimzey*, *supra,* 836 F.3d at p. 1269, fn.4 (internal quotation marks omitted) (quoting *Jones v. Dirty World Entertainment Recordings LLC* (6th Cir. 2014) 755 F.3d 398, 413–14). Here, recommending videos and selling advertisements may display and augment the illegal content, but it does not contribute to what makes it illegal. (See, e.g., *Dyroff, supra*, 934 F.3d at p. 1099 ["The recommendation and notification functions helped facilitate this user-to-user communication, but it did not materially contribute, as Plaintiff argues, to the alleged unlawfulness of the content."].)

Lastly, plaintiffs argue that defendants acted as information content providers in displaying verification badges which falsely identified hijacked channels as vetted and trustworthy. As explained below, we conclude that, while the SAC alleges defendants created the verification badges and materially contributed to the development of the

unlawful scam, the allegations are too conclusory to involve them in the creation or development of that content and make them information content providers under section 230. However, because there is a reasonable possibility that this defect could be cured by amendment, plaintiffs must be given leave to amend those particular claims.

i. Responsibility for creation or development of information

In certain circumstances, a website operator may be deemed responsible for creating or developing information, in whole or in part, under section 230. (§ 230, subd. (f)(3).)

A website operator is not deemed responsible for information merely because it compiled information voluntarily supplied by users. In *Gentry v. eBay, Inc.* (2002) 99 Cal.App.4th 816, the plaintiffs sued eBay, a website operator, after purchasing sports memorabilia on eBay that proved to be fake. They alleged eBay had violated Civil Code section 1739.7, which requires memorabilia dealers to provide certificates of authenticity to purchasers. (*Id*. at p. 826.) The court of appeal held that section 230 barred the claims because eBay merely published content provided by third parties who had falsely identified the items as authentic. (*Id*. at pp. 828-833.)

The court concluded eBay was not responsible for that content, based on a declaration from eBay and other documents of which the trial court had taken judicial notice demonstrating how eBay's website works. (*Id.* at pp. 831-832.) Because of that information, and concessions made by the plaintiffs, the court held that "the substance of appellants' allegations reveal [sic] they ultimately seek to hold eBay responsible for … eBay's dissemination of representations made by the [third parties], or the posting of compilations of information generated by those defendants and other third parties." (*Gentry*, 99 Cal.App.4th at p. 831.) Similarly, the court found that eBay was not responsible for the information in its ratings and "Power Sellers" designations for sellers

because those ratings and designations reflected "information provided by third party consumers and dealers." (*Id*. at p. 834.)

By contrast, in certain instances where website operators either create their own information or require users to supply information specified by the website, courts have held the operators responsible. (See *Roommates, supra,* 521 F.3d 1157; § 230, subd. (f)(3) [treating any person "responsible, in whole or in part, for the creation or development of information" as an "information content provider"].) In *Roommates,* a roommate-matching website required users to state their gender, sexual orientation, and familial status, and indicate whether they were willing to live with persons of various genders, sexual orientations, and familial status. (*Id.* at p. 1161.) It then posted this information on the users' profile pages and used it to determine which postings to show other users. (*Id*. at pp. 1161–1162, 1165.) Because the website itself required users to provide this information, the Ninth Circuit held the operator was partially responsible for the creation or development of the information, even though the specifics were supplied by third parties. (*Id*. at pp. 1165-1167.)

As the court explained, a website operator "can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is 'responsible, in whole or in part' for creating or developing, the website is also a content provider." (*Roommates, supra,* 521 F.3d at pp. 1162-1163.)

The court first held that "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." (*Roommates, supra,* 521 F.3d at p. 1165.) Further, with respect to the information ultimately provided by the users, the fact that they are "information content providers does not preclude Roommate from *also* being an information content provider by helping 'develop' at least 'in part' the information in the profiles." (*Ibid*.) Thus, in sharp contrast to websites that merely

provide "neutral tools" based on "voluntary inputs," the court observed, "Roommate's website is designed to force subscribers to divulge protected characteristics and discriminatory preferences." (*Id.* at p. 1172.)

Similarly, in *Liapes*, the First District Court of Appeal held that Facebook was responsible under section 230 for information used in advertisements on its website because the company required users to disclose that information. Much like the website in *Roommates*, Facebook required users to supply information to describe their age and gender. (*Liapes, supra,* 95 Cal.App.5th at p. 929.) It also required advertisers to select age and gender parameters, which were used, along with other parameters, to target ads. (*Ibid*.) Analogizing to *Roommates*, the court concluded that Facebook's ad-delivery tools did not "merely proliferate and disseminate content as a publisher"; they created, shaped, or developed that content. (*Id*. at p. 929, quoting *Roommates, supra*, 521 F.3d at pp. 1167-1168.)

In sum, existing precedent holds that where a website operator either creates its own content or requires users to provide information and then disseminates it, thereby materially contributing to the development of the unlawful information, it may be considered responsible for that information, and thus be an "information content provider." (§ 230, subd. (f)(3).)

The SAC here includes allegations potentially fitting within this category. For instance, it alleges that "YOUTUBE has continued to maintain the verification of channels that have been hijacked to broadcast BITCOIN GIVEAWAY scam videos and, in at least one instance, even issued a verification badge to a channel at the very time it was actively broadcasting scam videos."

It also alleges: "When YOUTUBE verifies a channel, YOUTUBE is communicating to its users that 'it's the official channel of a creator, artist, company, or public figure,' and that the channel 'represent[s] the real creator, brand, or entity it claims to be' because YOUTUBE has 'check[ed] different factors to help verify [the channel

owner's] identity.' YOUTUBE also verifies channels to 'distinguish official channels from other channels with similar names.' " Further, "YOUTUBE's users, including numerous Plaintiffs here, relied on YOUTUBE's representations that the verified channels are authentic and that the verification badge means the channel's owner is who they claim to be."

It can reasonably be inferred from these allegations that YouTube is wholly responsible for creating the information concerning the authenticity of the channel owners in the verification badges. Unlike the scam videos themselves, the third-party scammers did not create or develop the verification badges—defendants allegedly did. Nor is there any suggestion in the SAC that the verification badges contain information voluntarily provided by users and thus merely redirect or highlight third-party content. We therefore conclude the SAC adequately alleges that under section 230, YouTube is responsible for creating the information in the verification badges.

ii. Material Contribution

Despite these allegations, we cannot conclude that defendants are "information content providers" within the meaning of section 230 because the SAC, as currently pleaded, does not adequately allege that the information for which defendants are responsible gives rise to their asserted liability or materially contributed to the illegality of the conduct at issue.

Section 230 defines "information content provider" as a person responsible, in whole or in part, for "the creation or development" of information. (§ 230, subd. (f)(3)). Cases have long interpreted "creation" and "development" to require a "material contribution" to the alleged unlawfulness of the information at issue. (*Roommates*, *supra*, 521 F.3d at p. 1167-1168 ["We believe that both the immunity for passive conduits and the exception for co-developers must be given their proper scope and to that end we interpret the term 'development' as referring not merely to augmenting content generally, but to materially contributing to its alleged unlawfulness."]; see also *Kimzey*,

supra, 836 F.3d at p. 1269 [applying the material contribution requirement to "creation"].) "In other words, 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*, *supra*, 521 F.3d at p. 1168.)

The SAC asserts that the verification badges are "materially contributing to the criminally fraudulent enterprise that is the BITCOIN GIVEAWAY scam." Yet the SAC fails to allege specific facts showing *how* the badges materially contributed to the illegal conduct by plaintiffs. For instance, the first cause of action for misappropriation of likeness alleges in part that "Defendants' false or misleading statements include but are not limited to statements that … the scam videos were being aired by 'verified' or otherwise legitimate accounts or channels." However, the gravamen of the misappropriation claim is that the scammers used plaintiff Wozniak's name, likeness, and identity without his consent. The SAC does not explain how statements concerning verification of the accounts or channels materially contribute to the illegality of using that likeness without his consent. As a consequence, the verification badges provide no basis for treating defendants as the creator or developer of the content misappropriating plaintiff's Wozniak's likeness. It is well-settled that " 'conclusory allegations will not withstand demurrer.' " (*Fox v. Ethicon Endo-Surgery, Inc*. (2005) 35 Cal.4th 797, 808.)

Similarly, the second cause of action for fraud alleges that "Defendants falsely represented to Plaintiffs and their other users who viewed BITCOIN GIVEAWAY scam videos on YOUTUBE's website that… they were being broadcast by 'verified' or otherwise legitimate channels with large numbers of subscribers…." Further, it alleges scammers hijacked popular YouTube channels and falsely represented that the scam videos they were broadcasting were live and viewers were "liking" the videos.

However, these allegations do not demonstrate that the verification badges played any significant or meaningful role in conveying false impressions concerning the source or authenticity of the videos. Indeed, only seven of the 17 bitcoin plaintiffs even allege

that they relied on false verification of channels.[8] Moreover, it is unclear how many times defendants allegedly issued verification badges while a channel was broadcasting a scam video. Although the SAC alleges YouTube did so "in at least one instance," plaintiffs argue on appeal that "YouTube has also awarded channels that were actively running scam videos its 'verification badge,' " using the plural to suggest there were multiple instances. The SAC also does not specify whether defendants knew the channels had been hijacked, or whether the verifications were issued before or after the hijacking. Nor does it make clear which causes of action and theories of liability are predicated on the allegations regarding the verification badges. (*Liapes, supra,* 95 Cal.App.5th at p. 919 [to survive demurrer, plaintiff " 'must show the complaint alleges facts sufficient to establish every element of each cause of action' "].)

Accordingly, the SAC fails to provide a basis for concluding that defendants materially contributed to the illegal content and should be treated as the creators or developers of that content. (*Roommates, supra*, 521 F.3d at p. 1174 [close cases must be resolved in favor of immunity].)

3. Leave to amend

Nevertheless, the SAC's allegations regarding verification badges are sufficient to justify granting plaintiffs leave to amend, because there is a reasonable possibility that the infirmities we have discussed can be cured by amendment. (*Blank, supra,* 39 Cal.3d at p. 318.) In *Murphy,* the court explained in a section 230 context that " '[w]here the appellant offers no allegations to support the possibility of amendment and no legal authority showing the viability of new causes of action, there is no basis for finding the trial court abused its discretion when it sustained the demurrer without leave to amend.' " (*Murphy, supra,* 60 Cal.App.5th at p. 42, quoting *Total Call International, Inc. v.*

[8] The SAC alleges that the following bitcoin plaintiffs relied on false verifications: James Denitto, Bernardo Garcia, Jin Liu, Anthony Martinez, Myrielle Philistin, Daria Lopez Portilla, and Eric Restrepo.

Peerless Insurance Co. (2010) 181 Cal.App.4th 161, 173.) Here, though, we conclude plaintiffs have adequately alleged that defendants are responsible for the information in the verification badges, and although the SAC fails to allege that this information materially contributed to the illegal conduct or content from third parties, we cannot conclude there is no possibility of plaintiffs amending the complaint to do so.

We caution that we express no opinion regarding the viability of any claims in a subsequent amended complaint. We limit our conclusion as to the reasonable possibility of amendment solely to the allegations regarding verification badges.

B. Failure to state a claim for relief

Because the trial court ruled that section 230 provided immunity for all of plaintiffs' causes of action, it did not reach defendants' separate argument that the causes failed to state claims for relief. Defendants argue on appeal that, even if section 230 does not apply, this court should affirm on this alternative ground. Plaintiffs argue this court should instead remand to the trial court to decide the issue in the first instance.

Because we reverse and remand for plaintiffs to be given leave to amend as to their allegations regarding the verification badges, we need not reach this issue.

C. Discovery stay

The trial court based its denial of plaintiffs' motion to lift the discovery stay on the "significant public interest" of protecting websites from ultimate liability and from having to fight costly and protracted legal battles, and the importance of resolving immunity questions at the earliest possible stage in litigation to avoid unnecessary discovery and other burdens. The court also noted that "federal courts routinely stay discovery in cases apparently subject to Section 230 until the complaint is deemed adequate to avoid [section 230] immunity."

Those grounds have now shifted, and we remand for the trial court and the parties to consider the appropriate scope of discovery in light of our decision and subsequent developments in the trial court.

III. DISPOSITION

The judgment is reversed and the matter is remanded with directions to the trial court to enter a new order sustaining the demurrer with leave to amend, consistent with this opinion. In the interests of justice, the parties shall bear their own costs on appeal. (Cal. Rules of Court, rule 8.278(a)(5).)

_____
Wilson, J.

WE CONCUR:

_____
Danner, Acting P.J.

_____
Bromberg, J.

Wozniak et al. v. Youtube, LLC et al.
H050042

Trial Court:	Santa Clara County Superior Court No.: 20CV370338
Trial Judge: The Honorable Sunil R. Kulkarni	
Attorneys for Plaintiffs and Appellants Steve Wozniak et al.:	Joseph W. Cotchett Brian Danitz Christopher Owen Holleran Julia Qisi Peng Andrew F. Kirtley Gia Jung
Attorneys for Defendants and Respondents YouTube, LLC et al.:	David H. Kramer Amit Q. Gressel Carmen Sobczak Mark R Yohalem Ariel C. Green Anaba

Wozniak et al. v. YouTube, LLC et al.
H050042