UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: ZOOM VIDEO COMMUNICATIONS INC. PRIVACY LITIGATION

Case No. 20-CV-02155-LHK

ORDER GRANTING IN PART AND DENYING IN PART ZOOM'S MOTION TO DISMISS

Re: Dkt. No. 134

Plaintiffs, on behalf of themselves and two putative nationwide classes, allege that Defendant Zoom Video Communications, Inc. ("Zoom") violated nine provisions of California law. Plaintiffs specifically claim that Zoom violated California law by (1) sharing Plaintiffs' personally identifiable information with third parties; (2) misstating Zoom's security capabilities; and (3) failing to prevent security breaches known as "Zoombombing." Before the Court is Zoom's motion to dismiss Plaintiffs' first amended complaint. ECF No. 134. Having considered the parties' submissions; the relevant law; and the record in this case, the Court GRANTS IN PART and DENIES IN PART Zoom's motion to dismiss.

I. BACKGROUND

A. Factual Background

Zoom provides an eponymous video conference service that is available on computers, tablets, smartphones, and telephones. FAC ¶¶ 69–70. Since early 2020, the use of Zoom conferences (a.k.a. "Zoom meetings") has increased significantly in response to the COVID-19 pandemic. Today, Zoom has more than 200 million daily users. *Id.* ¶ 4.

Plaintiffs are Zoom users who allege—on behalf of themselves and two putative nationwide classes—that Zoom has made harmful misrepresentations and failed to secure Zoom meetings. Plaintiffs make three overarching allegations. *See* Opp'n at 1–3.

First, Plaintiffs allege that Zoom shared Plaintiffs' personally identifiable information ("PII") with third parties—such as Facebook, Google, and LinkedIn—without Plaintiffs' permission. This PII includes Plaintiffs' "device carrier, iOS Advertiser ID, iOS Device CPU Cores, iOS Device Display Dimension, iOS Device Model, iOS Language, iOS Time zone, iOS Version, even if the user did not have a Facebook account." Opp'n at 1 (citing FAC ¶¶ 5, 13, 78). This PII, "when combined with information regarding other apps used on the same device," allegedly allows third parties "to identify users and track their behavior across multiple digital services." FAC ¶¶ 88–89. Specifically, Plaintiffs allege this PII allows third parties to know when a particular device "open[s] or close[s]" Zoom. FAC ¶ 94. Third parties add this information about a particular device's Zoom usage to their fine-grained profiles on particular devices and people. FAC ¶ 95.

Second, Plaintiffs allege that "Zoom misstated the security capabilities and offerings of its services where Zoom failed to provide end-to-end encryption." Opp'n at 2 (citing FAC ¶¶ 7, 163–66). Specifically, Plaintiffs allege that Zoom misrepresents its encryption protocol—transport encryption—as end-to-end encryption. FAC ¶ 168. Transport encryption provides that "the encryption keys for each meeting are generated by Zoom's servers, not by the client devices." *Id.* Thus, Zoom can still access the video and audio content of Zoom meetings. *Id.* By contrast, end-to-end encryption provides that "the encryption keys are generated by the client (customer)

devices, and only the participants in the meeting have the ability to decrypt it." *Id.*

Plaintiffs' last overarching allegation is that Zoom has failed to prevent—and warn users about—security breaches known as "Zoombombing." A Zoom meeting is Zoombombed when bad actors join a meeting without authorization and "display[] pornography, scream[] racial epitaphs [sic], or engag[e] in similarly despicable conduct." FAC ¶ 9.

These three overarching allegations give rise to nine claims on behalf of all Plaintiffs and both putative classes: (1) invasion of privacy in violation of California common law and the California Constitution, Art. I, § 1; (2) negligence; (3) breach of implied contract; (4) breach of implied covenant of good faith and fair dealing; (5) unjust enrichment/quasi-contract; (6) violation of the California Unfair Competition Law, Cal. Bus. Prof. Code § 17200, *et seq.*; (7) violation of the California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*; (8) violation of the Comprehensive Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and (9) deceit by concealment under Cal. Civ. Code § 1710(3). Plaintiffs' two putative classes are:

> Nationwide Class: All persons in the United States who used Zoom.
>
> Under 13 Sub-Class: All persons under the age of 13 in the United States who used Zoom.

FAC ¶¶ 191–92.[1]

Plaintiffs are 11 individuals and two churches who have used Zoom. All Plaintiffs (except Saint Paulus Lutheran Church) allege that they relied on Zoom's promises that "(a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures." *E.g.*, FAC ¶¶ 18, 22, 26, 40, 57. In addition, six Plaintiffs, including the two churches, allege that they suffered Zoombombing in the following ways:

[1] "Specifically excluded from the Classes are Defendant and any entities in which Defendant has a controlling interest, Defendant's agents and employees, the judge to whom this action is assigned, members of the judge's staff, and the judge's immediate family." FAC ¶ 193.

- *Saint Paulus Lutheran Church* ("Saint Paulus") is an Evangelical Lutheran church located in San Francisco, California. FAC ¶ 32. Saint Paulus accesses Zoom video conferencing on an Apple laptop. *Id.* ¶ 31.

- *Heddi N. Cundle* is the administrator of Saint Paulus. Cundle uses Zoom both for Saint Paulus and herself. FAC ¶ 33. Cundle accesses Zoom video conferencing on her iPhone and Windows laptop. Cundle alleges that on May 6, 2020, she set up a password-protected Zoom meeting to hold a Bible study for Saint Paulus. *Id.* ¶ 37. Despite that password, an intruder hijacked the Zoom meeting and displayed child pornography. *Id.* Cundle then reported the Zoombombing incident to Zoom. *Id.* Zoom allegedly admitted that the intruder was "a known serial offender" who had "been reported multiple times to the authorities." *Id.* ¶ 37. Even so, Zoom allegedly did not ban the intruder from joining future meetings using the same Zoom software until Cundle reported the May 6, 2020 incident. *Id.*

- *Oak Life Church* ("Oak Life") is a non-denominational Christian church located in Oakland, California. FAC ¶ 39. Oak Life accesses Zoom video conferencing on an iPhone and Apple laptop on a paid Zoom Pro account. *Id.* On April 19, 2020, Oak Life set up a Sunday church service on Zoom with three security features: "a waiting room, mute on entry, and no ability for [non-host] users to share their screens." *Id.* ¶ 41. Despite these security features, an intruder hijacked the Zoom meeting and displayed child pornography. *Id.* The incident traumatized the meeting's participants and required Oak Life to hire trauma counsellors. *Id.*

- *Stacey Simins* is an operator of a burlesque dance studio and uses her Zoom Pro account for teaching classes. FAC ¶ 45. Simins accesses Zoom video conferencing on her iPhone, Apple laptop, or Apple desktop. *Id.* ¶ 43. Simins alleges that on "multiple occasions," uninvited men showed up to dance classes taught by her studio. *Id.* ¶ 45. The intrusion of these uninvited men has led to Simins losing 10 to 15 full-time members of her dance studio. *Id.*

- *Caitlin Brice* uses Zoom for speech therapy and to attend events. FAC ¶¶ 48–49. Brice accesses Zoom video conferencing on her Android phone, tablet, and Windows laptop. *Id.* ¶ 46. In April or May 2020, Brice alleges that she "attended a Zoom event during which the participants were subjected to intentional pornographic material when unknown men dropped into the meeting with the intention of disrupting it." *Id.* ¶ 49.

- *Peter Hirshberg* uses his Zoom Pro account to attend Zoom events. FAC ¶ 55. Hirschberg accesses Zoom video conferencing on his iPhone, iPads, and Apple computer. *Id.* ¶ 53. On May 30, 2020, Hirschberg alleges that he "attended a Zoom event during which the participants were subjected to intentional anti-semetic [sic] material when uninvited intruders dropped into the meeting with the intention of disrupting it." *Id.* ¶ 55.

Seven Plaintiffs do not allege Zoombombing. Rather, these Plaintiffs allege that Zoom shared their PII and misrepresented Zoom's encryption protocol. These seven Plaintiffs are the following individuals:

- *Kristen Hartmann* purchased a "Zoom Pro" account for her own personal use and accessed Zoom's video conferencing services on her iPhone. FAC ¶ 17. "After comparing Zoom against GoToMeeting and Webex, Ms. Hartmann selected Zoom over other options largely due to Zoom's representations of its end-to-end encryption. Further, periodically during Zoom meetings calls, Ms. Hartmann would 'check' to ensure the calls were end-to-end encrypted by hovering her cursor over the green lock icon in the application. . . . Had Ms. Hartmann known that Zoom meetings were not actually end-to-end encrypted, she would not have paid for a Zoom Pro subscription, or she would have paid less for it." FAC ¶¶ 18–19.
- *Isabelle Gmerek* has registered an account with Zoom and accesses Zoom's video conferencing services on her Android phone and iPad. FAC ¶ 21. "In late February or early March of 2020, Ms. Gmerek began using Zoom for meetings with her psychologist in reliance on representations by Zoom that it was a secure method of videoconferencing, that it was in full compliance with the Health Insurance Portability and Accountability Act ('HIPAA'), and that it had not misrepresented the security features available to users." FAC ¶ 23.
- *Lisa T. Johnston* has registered an account with Zoom and uses Zoom videoconferencing on her Apple laptop and iPhone. FAC ¶ 25. Johnston generally alleges, as all Plaintiffs but Saint Paulus do, that she relied on Zoom's promises that "(a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures." *Id.* ¶ 26.
- *M.F.* is a minor who was under the age of 13 at all relevant times. *Id.* ¶ 27. M.F. accesses Zoom video conferencing on an iPad, Windows laptop, and Android phone. *Id.* ¶ 28. Like Johnston and other Plaintiffs, M.F. makes general allegations about reliance. *Id.*
- *Therese Jimenez* is the mother and guardian of M.F. FAC ¶ 29. Jimenez accesses Zoom video conferencing on her iPad, Windows laptop, and Android phone. *Id.* Like M.F. and other Plaintiffs, Jimenez makes general allegations about reliance. *Id.* ¶ 30.
- *Sharon Garcia* purchased a Zoom Pro account for her personal use. FAC ¶ 56. She accesses Zoom video conferencing on her iPhone, Windows laptop, and tablet. *Id.* Like Jimenez and other Plaintiffs, Garcia makes general allegations about reliance. *Id.* ¶ 57.
- *Angela Doyle* makes the same allegations as Garcia, except that Doyle alleges accessing Zoom on slightly different devices: an iPhone and Windows computer. FAC ¶ 58.

Lastly, one former Plaintiff, Cynthia Gormezano, alleged using Zoom on her iPhone in March 2020—earlier than other Plaintiffs. FAC ¶¶ 50–52. However, on February 18, 2021, Gormezano voluntarily dismissed her claims against Zoom. ECF No. 158.

B. Procedural History

On March 30, 2020, a plaintiff named Robert Cullen (who is not a Plaintiff in the operative complaint) filed a class action complaint against Zoom. ECF No. 30. Cullen's lawsuit was assigned the instant case number, 20-CV-02155. On May 28, 2020, the Court consolidated 13 other lawsuits under 20-CV-02155. ECF No. 62. On July 30, 2020, Plaintiffs filed a consolidated class action complaint. ECF No. 114. Zoom moved to dismiss that complaint, but before the Court could rule, the parties stipulated to Plaintiffs' filing of the operative First Amended Consolidated Class Action Complaint ("FAC"). ECF No. 115.

Plaintiffs filed the FAC on October 28, 2020. ECF No. 126. Zoom filed the instant motion to dismiss the FAC on December 2, 2020. ECF No. 134 ("Mot."). Plaintiffs filed their opposition to Zoom's instant motion on December 30, 2020. ECF No. 141 ("Opp'n"). Zoom filed its reply on January 21, 2021. ECF No. 147 ("Reply").[2]

[2] Zoom requests judicial notice of six exhibits. ECF No. 134-1. Exhibit 1 is Zoom's Terms of Service. *Id.* at 3. Exhibits 2 to 6 are versions of Zoom's Privacy Statement, with effective dates ranging from the present to February 23, 2020. *Id.* Zoom's request is unopposed as to Exhibits 3, 4, and 6. ECF No. 141-1. The Court may take judicial notice of matters that are either "generally known within the trial court's territorial jurisdiction" or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). Moreover, courts may consider materials referenced in the complaint under the incorporation by reference doctrine, even if a plaintiff failed to attach those materials to the complaint. *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005). Public terms of service and privacy policies are proper subjects of judicial notice. *See, e.g.*, *Coffee v. Google, LLC*, No. 20-CV-03901-BLF, 2021 WL 493387, at *3 (N.D. Cal. Feb. 10, 2021) (noticing Google's terms of service). Accordingly, the Court GRANTS Zoom's request for judicial notice, ECF No. 134-1. However, the Court only takes "judicial notice of the fact that these documents exist, 'not whether, for example, the documents are valid or binding contracts.'" *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 975 (N.D. Cal. 2015) (quoting *Datel Holdings Ltd. v. Microsoft Corp.*, 712 F. Supp. 2d 974, 984 (N.D. Cal. 2010)).

II. LEGAL STANDARD

A. Motion to Dismiss Under Rule 12(b)(6)

Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). The United States Supreme Court has held that Rule 8(a) requires a plaintiff to plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "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." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id*. (internal quotation marks omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). The Court, however, need not "assume the truth of legal conclusions merely because they are cast in the form of factual allegations." *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (internal quotation marks omitted). Additionally, mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

B. Leave to Amend

If a court determines that a complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend "shall be freely given when justice so requires," bearing in mind "the underlying purpose of Rule 15 to facilitate decisions on the merits, rather than on the pleadings or technicalities." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (alterations and internal quotation marks omitted). When dismissing a complaint for failure to state a claim, "a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the

pleading could not possibly be cured by the allegation of other facts." *Id.* at 1130 (internal quotation marks omitted).

Accordingly, leave to amend generally shall be denied only if allowing amendment would unduly prejudice the opposing party, cause undue delay, or be futile, or if the moving party has acted in bad faith. *Leadsinger, Inc. v. BMG Music Publ'g*, 512 F.3d 522, 532 (9th Cir. 2008). At the same time, a court is justified in denying leave to amend when a plaintiff "repeated[ly] fail[s] to cure deficiencies by amendments previously allowed." *See Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 892 (9th Cir. 2010). Indeed, a "district court's discretion to deny leave to amend is particularly broad where plaintiff has previously amended the complaint." *Cafasso, U.S. ex rel. v. Gen. Dynamics C4 Sys., Inc.*, 637 F.3d 1047, 1058 (9th Cir. 2011) (quotation marks omitted).

III. DISCUSSION

The FAC pleads nine claims on behalf of all Plaintiffs and two putative nationwide classes: (1) invasion of privacy in violation of California common law and the California Constitution, Article I, § 1; (2) negligence; (3) breach of implied contract; (4) breach of implied covenant of good faith and fair dealing; (5) unjust enrichment/quasi-contract; (6) violation of the California Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200, *et seq.*; (7) violation of the California Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code § 1750, *et seq.*; (8) violation of the Comprehensive Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and (9) deceit by concealment under Cal. Civ. Code § 1710(3).

Zoom moves to dismiss all claims with prejudice. Mot. at 25. To support its motion, Zoom first makes two overarching arguments. First, Zoom argues that § 230(c)(1) of the Communications Decency Act bars Plaintiff' claims to the extent the claims are based on "Zoombombing." Mot. at 4–6. Second, Zoom groups the claims together and argues that Plaintiffs categorically fail to allege harm under any claim. Zoom then specifically challenges each claim. Zoom analyzes the three "fraud-based" claims—the UCL, CLRA, and fraudulent concealment claims—together. Mot. at ii.

The Court first addresses Zoom's § 230(c)(1) immunity argument. Then, the Court

analyzes the claims in the same order as the parties: invasion of privacy (Count 1); negligence (Count 2); breach of implied contract (Count 3); breach of implied covenant of good faith and fair dealing (Count 4); violation of the CDAFA (Count 8); fraud-based claims (Counts 6, 7, and 9); and unjust enrichment/quasi-contract (Count 5). Whether Plaintiffs have adequately alleged harm is analyzed as to each claim.

A. Section 230(c)(1) of the Communications Decency Act partially bars Plaintiffs' claims to the extent they are based on Zoombombing.

Zoom's first overarching argument is that § 230(c)(1) of the Communications Decency Act, 47 U.S.C. § 230, bars Plaintiffs' claims to the extent they are based on third parties disrupting Plaintiffs' Zoom meetings ("Zoombombing"). Mot. at. 4–8. The Court agrees with Zoom in part.

As a general matter, § 230 "immunizes providers of interactive computer services against liability arising from content created by third parties." *Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1162 (9th Cir. 2008) (en banc). The text of § 230(c)(1) specifically provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). Pursuant to this statutory text, the Ninth Circuit has set forth a three-element test for a defendant to receive § 230(c)(1) immunity. Section 230(c)(1) "only protects from liability (1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat . . . as a publisher or speaker (3) of information provided by another information content provider." *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1100–01 (9th Cir. 2009), *as amended* (Sept. 28, 2009).

Here, "Plaintiffs do not dispute that the allegedly harmful content at issue was posted by third parties and that Zoom played no role in authoring it." Reply at 2. The parties instead dispute whether Zoom meets the first two elements of § 230(c)(1)'s test. *See* Mot. at 4–8; Opp'n at 3–4. The Court concludes that Zoom meets the first element of § 230(c)(1). However, as to the second element, Plaintiffs do not treat Zoom as a "publisher or speaker" with respect to all claims. Thus, as explained below, Zoom is partially immune Plaintiffs' Zoombombing claims.

1. Zoom is an interactive computer service.

Plaintiffs argue that Zoom is not an interactive computer service. Opp'n at 4. Plaintiffs reason that Zoom is not a *public* platform. *Id.* at 3. "Rather, Zoom calls are intended to involve only the invited participants for a finite duration." *Id.* at 4.

Zoom responds with two arguments. First, Zoom argues that it clearly meets the statutory definition of "interactive computer service." Mot. at 5–6. Second, Zoom argues that Plaintiffs' public-private distinction is factually and legally flawed. Factually, some Zoom meetings are open to the public. Reply at 2 n.2. As for the law, Zoom argues that the case law supports granting § 230(c)(1) immunity even to Zoom's transmission of *nonpublic* messages in meetings limited to invited participants. *Id.* at 2. The Court agrees with Zoom and addresses each argument in turn.

First, Zoom meets the definition of "interactive computer service." In general, courts "interpret the term 'interactive computer service' expansively." *Dyroff v. Ultimate Software Grp., Inc.*, 934 F.3d 1093, 1097 (9th Cir. 2019) (quoting *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1268 (9th Cir. 2016)), *cert. denied*, 140 S. Ct. 2761 (2020). Courts' expansive interpretations track the expansive statutory text. Specifically, § 230(f)(2) provides that an "interactive computer service" is "*any* [1] information service, system, or *access software provider* that [2] *provides or enables computer access by multiple users to a computer server*." 47 U.S.C. § 230(f)(2) (emphasis added).

The undisputed facts show that Zoom meets both parts of the statutory definition. To start, Zoom is an "access software provider." *Id.* "Access software provider[s]" include "provider[s] of software" that "transmit, receive, display, [or] forward . . . content." *Id.* § 230(f)(4). Zoom provides software that undisputedly transmits and displays video, audio, and written content. *See, e.g.*, FAC ¶¶ 64–65 (describing Zoom as a communications platform for video, audio, and messaging).

Zoom also "provides or enables computer access by multiple users to a computer server." 47 U.S.C. § 230(f)(2). It is undisputed that Zoom enables multiple users to access a computer server. The FAC specifically alleges that "Zoom is a supplier of video conferencing services" that hosts a connection "between [1] the Zoom app running on a user's computer or phone and

[2] Zoom's server." FAC ¶¶ 2, 168. Thus, Zoom plainly meets the statutory definition of "interactive computer service."

Second, case law confirms that Zoom is an interactive computer service. As both the Ninth and Tenth Circuits have explained, the "prototypical service qualifying for [§ 230] immunity is an online messaging board" on which users "post comments and respond to comments posted by others." *Kimzey*, 836 F.3d at 1266 (quoting *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1195 (10th Cir. 2009)). Zoom is the video equivalent of an online messaging board. Users converse in real-time—and may use Zoom's built-in chat feature too. *See, e.g.*, FAC ¶¶ 151–52 (discussing video conferences and chats). Accordingly, the Court finds that Zoom is an interactive computer service.

Plaintiffs' response is that "Zoom calls are intended to involve only the invited participants." Opp'n at 4. This response is factually overbroad and legally imprecise. Factually, many Zoom meetings are open to the public. Legally, the public/private nature of a meeting is immaterial to whether Zoom is an "interactive computer service." Section 230 requires merely that Zoom "provides or enables computer access by multiple users to a computer server." 47 U.S.C. § 230(f)(2). Likewise, the case law does not recognize a public/private distinction. Section 230 immunity can also "bar claims predicated on a defendant's transmission of *nonpublic* messages." *Fields v. Twitter, Inc.*, 217 F. Supp. 3d 1116, 1128 (N.D. Cal. 2016) (emphasis added), *aff'd*, 881 F.3d 739 (9th Cir. 2018). For instance, the *Fields* Court dismissed claims that sought to hold Twitter liable for private messages sent using Twitter's "Direct Messaging" feature. *Id.* Following at least three other courts, the *Fields* Court held that "the private nature" of messaging was immaterial. *Id.* (collecting cases).

In sum, it is irrelevant whether a message is directed at one recipient (like in Direct Messaging); a small group (like in an AOL chat room); or the public (like in messaging boards). The relevant question is whether an "interactive computer service" transmitted that message. The statutory text and case law show that Zoom is an interactive computer service.

2. Some of Plaintiffs' claims seek to treat Zoom as a publisher or speaker of third-party content.

The other challenged element of § 230(c)(1) immunity is whether Plaintiffs' Zoombombing claims seek to treat Zoom as a "publisher or speaker." *Barnes*, 570 F.3d at 1101. Plaintiffs argue that they "seek to hold Zoom accountable for its failure to provide promised security and privacy during Zoom calls, not for Zoom's actions as a content provider, publisher, or speaker." Opp'n at 4 (citing FAC ¶¶ 177, 180–82). Zoom responds that "[c]ourts routinely reject such attempts to skirt Section 230." Reply at 3.

The Court agrees with Zoom in part. As explained below, Section 230(c)(1) largely bars Plaintiffs' claims. For instance, Plaintiffs cannot hold Zoom liable for injuries stemming from the heinousness of third-party content. *See, e.g.*, FAC ¶ 179 (challenging "disturbing display" of images). These claims (1) challenge the harmfulness of "content provided by another"; and (2) "derive[] from the defendant's status or conduct as a 'publisher or speaker'" of that content. *Barnes*, 570 F.3d at 1102. However, § 230(c)(1) otherwise allows Plaintiffs' claims. For instance, Plaintiffs may claim that Zoom breached contractual duties because these duties are independent of Zoom's role as "publisher or speaker." *See* FAC ¶¶ 224–43 (implied contract and implied covenant claims). Supporting this conclusion are § 230's text, legislative history, and case law. The Court analyzes each authority in turn.

a. Section 230(c)'s text encourages and immunizes content moderation, not security failures.

To start, the text of § 230(c) immunizes the "blocking and screening of offensive material," not failures to secure software from intrusion. The "blocking and screening of offensive material" is also known as "content moderation." For example, the Ninth Circuit, like many commentators, has called the blocking and screening of offensive material "content moderation." *Prager Univ. v. Google LLC*, 951 F.3d 991, 996 (9th Cir. 2020); *see also, e.g.*, U.S. Dep't of Justice, *Section 230—Nurturing Innovation or Fostering Unaccountability?* at 4 (June 2020) (stating that § 230(c) immunizes "content moderation").

Three parts of the text highlight the distinction between content moderation and security

failures. The first is the caption of § 230's immunity provision, § 230(c). The caption reads: "Protection for 'Good Samaritan' blocking and screening of offensive material." 47 U.S.C. § 230(c). The caption underscores that § 230(c) immunizes affirmative, good-faith acts. *See Doe v. Internet Brands, Inc.*, 824 F.3d 846, 852 (9th Cir. 2016) (noting same). As the en banc Ninth Circuit has held, "the substance of section 230(c) can and should be interpreted consistent with its caption." *Roommates.Com, LLC*, 521 F.3d at 1164.

The two subsections of § 230(c) continue this theme of immunizing affirmative content moderation. Subsection 230(c)(2) immunizes "any action voluntarily taken in good faith to restrict access to" objectionable content. *Id.* § 230(c)(2). In turn, § 230(c)(1)—the provision disputed by the parties here—provides that "[n]o provider or user of an interactive computer service shall be treated as the *publisher or speaker* of any information provided by another information content provider." *Id.* § 230(c)(1) (emphasis added). Thus, an interactive computer service can moderate third-party content without fear that it will "be treated as the "publisher or speaker of" that content.

The last relevant part of the text is § 230's declarations of policy. Section 230(b) declares the policy of the United States is to *encourage* content moderation—not to provide immunity so broad that content moderation becomes disincentivized. Specifically, § 230(b)(3) "encourage[s] the development of technologies which *maximize user control* over what information is received by individuals, families, and schools who use the Internet and other interactive computer services." *Id.* § 230(b)(3) (emphasis added). Similarly, § 230(b)(4) seeks "to remove disincentives for the development and utilization of *blocking and filtering technologies* that empower parents to restrict their children's access to objectionable or inappropriate online material." *Id.* § 230(b)(4) (emphasis added). These declarations of policy support the security-based subset of Plaintiffs' claims. "[M]aximiz[ing] user control over what information is received" would include preventing—not allowing—unauthorized intrusions into private meetings. Likewise, "utilization of blocking and filtering technologies" would help prevent unauthorized intrusions.

b. Section 230's legislative history also states that § 230's purpose is to encourage and immunize content moderation.

Section 230's legislative history echoes its statutory text. The bicameral Conference Report summarized § 230 as a provision immunizing affirmative content moderation:

> This section provides ''Good Samaritan'' protections from civil liability for providers or users of an interactive computer service for actions *to restrict or to enable restriction of access* to objectionable online material. One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy*[, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)] and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own *because they have restricted access* to objectionable material. The conferees believe that such decisions create serious obstacles to the important federal policy of *empowering parents to determine the content of communications* their children receive through interactive computer services.

S. Rep. No. 104-230, at 194 (1996) (emphasis added).

Based on this Conference Report, the en banc Ninth Circuit has held that "perhaps the only purpose" of § 230 is "to immunize the *removal* of user-generated content." *Roommates.Com*, 521 F.3d at 1163 & n.12 (emphasis in original); *see also Force v. Facebook, Inc.*, 934 F.3d 53, 77–80 (2d Cir. 2019) (Katzmann, C.J., concurring in part and dissenting in part) (summarizing § 230's legislative history). Missing from the Conference Report is any intention to immunize conduct unrelated to content moderation, such a failure to protect users from a security breach.

c. The case law implements § 230 by only immunizing claims that (1) challenge the harmfulness of content provided by another; and (2) do not derive from defendant's status or conduct as a publisher or speaker.

Given § 230's text and legislative history, courts have held that "the [Communications Decency Act] does not declare 'a general immunity from liability deriving from third-party content.'" *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 852 (9th Cir. 2016) (quoting *Barnes*, 570 F.3d at 1100). Rather, "§ 230 bars 'lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content.'" *FTC v. LeadClick Media, LLC*, 838 F.3d 158, 174 (2d Cir. 2016) (quoting *Jones v. Dirty World Ent. Recordings LLC*, 755 F.3d 398, 407 (6th Cir. 2014)). Broader immunity would defeat § 230(c)'s purpose. If § 230(c) "provide[d] equal protection as

between internet service providers who do nothing and those who attempt to block and screen offensive material . . . then 'internet service providers may be expected to take the do-nothing option and enjoy immunity' because 'precautions are costly.'" *Barnes*, 570 F.3d at 1105 (original alterations omitted) (quoting *Doe v. GTE Corp.*, 347 F.3d 655, 660 (7th Cir. 2003)).

Specifically, § 230(c)(1) immunity only extends to certain claims: claims that "*inherently require*[] the court to treat the defendant as the '*publisher or speaker*' of *content provided by another*." *Id.* at 1102 (emphasis added). The *Barnes* Court sketched the contours of this rule with several examples of immunized claims. A defamation claim is the paradigmatic example. *Id.* at 1101. Congress enacted § 230 "in part to respond to a New York state court decision, *Stratton Oakmont*, which held that an internet service provider could be liable for defamation." *Id.* (citation shortened). Other immunized claims include those for "false light"—which penalize falsehoods that inflict emotional distress—and "negligent publication of advertisements that cause harm to third parties." *Id.* (citing *Flowers v. Carville*, 310 F.3d 1118, 1132 (9th Cir. 2002); and *Braun v. Soldier of Fortune Magazine, Inc.*, 968 F.2d 1110 (11th Cir. 1992)).

These immunized claims, as *Barnes* and other cases show, all meet two conditions. First, these claims challenge the *harmfulness* of "content provided by another." *Id.* Second, these claims allege violations of a duty that does *not* "derive[] from the defendant's status or conduct as a 'publisher or speaker.'" *Id.* Thus, § 230(c)(1) allows two types of claims: claims that either (1) are content-neutral; or (2) do not derive from defendant's status or conduct as a publisher or speaker. The Court analyzes each type of non-immunized claim in turn.

i. Section 230(c)(1) allows content-neutral claims.

Content-neutral claims do not challenge the harmfulness of third-party content on defendant's platform. It is irrelevant to these claims whether third-party content on defendant's platform is good or bad, displayed or hidden. Rather, liability stems from a content-neutral rule. Three examples from this circuit illustrate what constitutes a content-neutral claim allowed by § 230(c)(1).

First, the Ninth Circuit held that § 230(c)(1) immunity did not apply to content-neutral

liability. Specifically, in *HomeAway.com vs. City of Santa Monica*, an ordinance required short-term rental platforms (such as Airbnb) to "refrain[] from completing any booking transaction for properties not licensed and listed on the City's registry." 918 F.3d 676, 680 (9th Cir. 2019). The rental platforms argued that § 230(c)(1) preempted the ordinance. The rental platforms specifically argued that the ordinance impermissibly required them to "monitor the content of a third-party listing and compare it against the City's short-term rental registry." *Id.* at 682.

The Ninth Circuit disagreed. The Ninth Circuit reasoned that the ordinance does not "even discuss the content of the listings that the Platforms display on their websites. It requires only that transactions involve licensed properties." *Id.* at 683 (citation omitted). In other words, the ordinance allows the posting of unlicensed properties, but bans the *booking* of such properties. The rental platforms "face *no liability for the content* of the bookings." *Id.* at 684 (emphasis added). Thus, § 230(c)(1) allows the ordinance. *Id.*; *accord Dyroff*, 934 F.3d at 1098 (summarizing *HomeAway.com*).

Second, in *Nunes v. Twitter*, 194 F. Supp. 3d 959, 968 (N.D. Cal. 2016), the court held that where a statute imposes liability regardless of content, § 230(c)(1) immunity does not apply. *Nunes* involved the Telephone Consumer Protection Act ("TCPA"), which strictly proscribes texts sent without the recipient's consent—regardless of "whether the content of the unwanted t[ext]s is bad or good, harmful or harmless." *Nunes*, 194 F. Supp. 3d at 968; *see, e.g.*, *Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 955 (9th Cir. 2009) (summarizing TCPA's text ban). In *Nunes*, Twitter texted tweets authored by a former Magistrate Judge to a plaintiff who had not agreed to receive Twitter's texts. *Id.* at 961. The Magistrate Judge's tweets were benign. *Id.* at 960. Even so, Twitter was liable for texting plaintiff without plaintiff's consent. *Id.* at 968. The text itself—not its content—violated the TCPA. *Id.* Thus, because the TCPA is content-neutral, § 230(c)(1) did not immunize Twitter from liability. *Id.*; *accord Cunningham v. Montes*, 378 F. Supp. 3d 741, 750 (W.D. Wis. 2019) (adopting *Nunes* to unwanted phone calls).

Lastly, the Ninth Circuit has held that where a claim does not challenge any third-party content on defendant's platform, § 230(c)(1) immunity does not apply. Specifically, in *Doe v.*

Internet Brands, plaintiff Jane Doe did not challenge any third-party content on Internet Brand's website. *See Internet Brands*, 824 F.3d at 849 (factual background). Rather, Doe challenged Internet Brands' failure to warn her that criminals were browsing Internet Brands "to identify targets for a rape scheme." *Id.* at 848. These criminals would then contact their targets offline, or at least not through Internet Brands. At no point did the criminals "post[] their own profiles on the website" nor make "any posting that Internet Brands failed to remove." *Id.* at 848, 851. Thus, the Ninth Circuit reasoned that Doe's claim would not necessarily "require Internet Brands to remove any user content." *Id.* at 851. Doe simply wanted Internet Brands "to generate its own warning" about an evil unrelated to Internet Brands' content. *Id.* at 852.

All these cases show that § 230(c)(1) allows content-neutral claims: claims that do not challenge the harmfulness of third-party content on defendant's platform. These claims are the first type of claims allowed by § 230(c)(1).

ii. Section 230(c)(1) allows claims that do not derive from defendant's status or conduct as a "publisher" or "speaker".

Section 230(c)(1) also allows a second type of claims: a subset of claims that are not content-neutral. These claims do not "derive[] from the defendant's status or conduct as a 'publisher or speaker.'" *Barnes*, 570 F.3d at 1102. Contract claims are such claims under Ninth and Third Circuit precedent. The Court analyzes each circuit's precedent in turn.

In *Barnes v. Yahoo!*, plaintiff Cecilia Barnes alleged that she had relied on "Yahoo's 'promise' to remove [] indecent profiles." *Barnes*, 570 F.3d at 1099. Barnes's claim thus was content-based. It potentially required examining and removing Yahoo profiles that were "indecent." Even so, the Ninth Circuit held that "insofar as Barnes alleges a breach of contract claim under the theory of promissory estoppel, [§] 230(c)(1) of the [Communications Decency] Act does not preclude her cause of action." *Id.* at 1109. The Ninth Circuit reasoned that "[c]ontract liability [] would come not from Yahoo's publishing conduct, but from Yahoo's manifest intention to be legally obligated to do something, which happens to be removal of material from publication." *Id.* at 1107. Simply put, Yahoo's alleged contract with Barnes had "generate[d] legal

duty distinct from" Yahoo's status as publisher. *Id.*

Like Barnes, the plaintiff in *Green v. America Online (AOL)*, 318 F.3d 465 (3d Cir. 2003), raised a contract claim. Plaintiff John Green argued that AOL had contractually promised to "protect Green from other subscribers" who had messaged him a virus and defamed him. *Id.* at 471. Given this purported promise, Green argued that AOL had "waived its immunity under [S]ection 230." *Id.*

The Third Circuit did not dispute that AOL's contracts could waive § 230 immunity. The Third Circuit merely held that, by the terms of AOL's contracts, "AOL did not promise to protect Green from the acts of other subscribers." *Id.* at 472. Thus, like the Ninth Circuit in *Barnes*, the Third Circuit allowed the possibility of contractual claims despite § 230(c)(1).

In sum, § 230's text, legislative history, and case law all show that § 230(c)(1) "does not declare 'a general immunity from liability deriving from third-party content.'" *Internet Brands*, 824 F.3d at 852 (quoting *Barnes*, 570 F.3d at 1100). Section 230(c)(1) instead immunizes liability deriving from *moderation* of third-party content. This immunity covers claims that (1) challenge the harmfulness of "content provided by another"; and (2) "derive[] from the defendant's status or conduct as a 'publisher or speaker'" of that content. *Barnes*, 570 F.3d at 1102. Conversely, § 230(c)(1) *allows* claims that either (1) are content-neutral; or (2) do not derive from defendant's status or conduct as a publisher or speaker.

d. Section 230(c)(1) mostly immunizes Zoom from Plaintiffs' Zoombombing claims here.

Given these principles, Section 230(c)(1) mostly immunizes Zoom from Plaintiffs' Zoombombing claims here. The Zoombombing claims largely (1) challenge the harmfulness of specific content provided by third parties; and (2) allege that Zoom should have done more to moderate or block that harmful content. Specifically, Plaintiffs claim that "failures of Zoom's security protocols" allowed unauthorized participants to disrupt Zoom meetings with "racial slurs and other derogatory statements." FAC ¶¶ 173, 177. The harmful third-party content at issue comprised (1) child pornography, FAC ¶¶ 37, 41; (2) "several minutes" of video and/or audio from

uninvited men, *id.* ¶ 45; (3) "intentional pornographic material," *id.* ¶ 49; and (4) "intentional anti-semetic [sic] material," *id.* ¶ 55. *See* Section I-A, *supra* (detailing six Plaintiffs who allege Zoombombing). The depravity of the child pornography in particular "was beyond description." FAC ¶ 37.

Plaintiffs exposed to this user-generated content suffered emotional distress as a result. *Id.* ¶ 221. Yet, appalling as this content is, Zoom's failure "to edit or block user-generated content" is "the very activity Congress sought to immunize." *Roommates.Com*, 521 F.3d at 1172 n.32. The bulk of Plaintiffs' Zoombombing claims lie against the "Zoombombers" who shared heinous content, not Zoom itself. Zoom merely "provid[ed] neutral tools for navigating" its service. *Id.* at 1174 n.37; *see, e.g.*, FAC ¶ 177 (criticizing Zoom's "default features").

In sum, the Court rules as follows on § 230(c)(1) immunity. The Court denies Zoom's motion to dismiss Plaintiffs' contract claims. These claims do not derive from Zoom's status or conduct as a "publisher" or "speaker." The Court also denies Zoom's motion to dismiss Plaintiffs' claims to the extent they are content-neutral. Plaintiffs' second amended complaint should more clearly articulate those claims.

The Court grants Zoom's motion to dismiss Plaintiffs' claims to the extent they (1) challenge the harmfulness of "content provided by another"; and (2) "derive[] from the defendant's status or conduct as a 'publisher or speaker'" of that content. *Barnes*, 570 F.3d at 1102. However, the Court allows Plaintiffs leave to amend because amendment would not unduly prejudice the opposing party, cause undue delay, or be futile, and Plaintiffs have not acted in bad faith. *See Leadsinger*, 512 F.3d at 532.

B. Count 1: Plaintiffs inadequately plead an invasion of privacy under California law.

Zoom argues that Plaintiffs fail to state a claim for invasion of privacy under California law. Zoom offers three reasons why. First, Zoom argues that "Plaintiffs do not allege that Zoom disseminated or misused any of *their* information to a third party—such as using the iOS app" that implemented the Facebook software development kit ("SDK"). Reply at 4 (emphasis in original).

Second, Zoom argues that "courts regularly dismiss invasion of privacy claims at the pleading stage where, as here, the alleged information is not sensitive." *Id.* at 5. Third, Zoom argues that the two institutional Plaintiffs—Saint Paulus Lutheran Church ("Saint Paulus") and Oak Life Church ("Oak Life")—lack privacy rights under either California common law or the California Constitution. *Id.* at 6.

Plaintiffs disagree with Zoom on all grounds. First, Plaintiffs argue that they have in fact alleged that Zoom shared their personal data. Opp'n at 6. Second, Plaintiffs argue that two cases show that Plaintiffs have "a reasonable expectation of privacy in the information Zoom [allegedly] shared without their permission." *Id.* at 7 (discussing *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 603–04 (9th Cir. 2020), and *Carpenter v. United States*, 138 S. Ct. 2206 (2018)). Third, Plaintiffs argue that the institutional Plaintiffs have privacy rights under *H&M Assocs. v. City of El Centro*, 109 Cal. App. 3d 399, 410 (1980). *Id.* at 6 n.3.

The Court agrees with Zoom that Plaintiffs have failed to allege that *Plaintiffs*' data was shared with a third party. The Court analyzes this failure to allege harm below. Because this failure is dispositive, the Court need not address Zoom's other two arguments on the sensitivity of data or institutional Plaintiffs.

Plaintiffs allege that Zoom shared Plaintiffs' data in three ways: (1) through the Facebook SDK implemented on pre-March 27, 2020 versions of Zoom's iOS app, FAC ¶ 78; (2) through Zoom's Android app, "depending on the smartphone and operating system," FAC ¶¶ 110, 128; and (3) through "a LinkedIn service for sales prospecting, called LinkedIn Sales Navigator"—assuming Plaintiffs had been in a Zoom meeting with another user who subscribed to LinkedIn Sales Navigator, FAC ¶ 123.

The Court analyzes each method of alleged data sharing in turn. In doing so, the Court looks for whether Plaintiffs have made more than "bare allegation[s] that each [] Plaintiff 'interacted with' their device 'repeatedly.'" *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 817 (N.D. Cal. 2020) (citing *Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026, 1035 (N.D. Cal. 2014)). Merely using a device or app repeatedly is insufficient to plead an invasion of privacy

under California law. *See id.* at 828–30 (collecting cases). Plaintiffs must instead allege facts that plausibly show that Plaintiffs' private data was disclosed, such as facts "regarding the participants in the conversations, the locations of the conversations, or examples of content from the conversations" in which Plaintiffs' private data was disclosed. *Id.* at 817; *accord, e.g.*, *Banga v. Equifax Info. Servs. LLC*, No. 14-CV-03038-WHO, 2015 WL 3799546, at *9 (N.D. Cal. June 18, 2015) (requiring plaintiff to allege "what particular information was disclosed"); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (requiring same). As discussed below, Plaintiffs fail to adequately plead these facts.

1. Plaintiffs inadequately allege that Zoom shared their personal data through Facebook's SDK.

The Court first analyzes Plaintiffs' allegations on Zoom's implementation of the Facebook SDK. The Court concludes that one former Plaintiff may have adequately alleged that Zoom shared her personal data through the Facebook SDK. Specifically, former Plaintiff Cynthia Gormezano alleges using Zoom on an iPhone "in March of 2020," FAC ¶ 52—which is likely while Zoom's iOS app still implemented Facebook's SDK. Zoom removed Facebook's SDK from its iOS app on March 27, 2020. *See* FAC ¶ 78 (citing Eric S. Yuan, *Zoom's Use of Facebook's SDK in iOS Client* (Mar. 27, 2020), https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/). Versions of Zoom's iOS app pre-dating March 27, 2020 shared the following data with Facebook about *each* device running Zoom's iOS app:

> Application Bundle Identifier; Application Instance ID; Application Version; Device Carrier; iOS Advertiser ID; iOS Device CPU Cores; iOS Device Disk Space Available; iOS Device Disk Space Remaining; iOS Device Display Dimensions; iOS Device Model; iOS Language; iOS Timezone; iOS Version; and IP Address.

Id. Facebook allegedly uses this information to help identify (or "fingerprint") specific devices, which allows Facebook to link a device's Zoom usage with other information Facebook knows about that device. *See, e.g.*, FAC ¶ 88. Gormezano's pre-March 27, 2020 use of Zoom "for meetings with her [physical therapy] patients" therefore would have shared "fingerprint" data about Gormezano's iPhone with Facebook. *Id.* ¶ 52.

However, on February 18, 2021, Gormezano voluntarily dismissed her claims against Zoom without prejudice. ECF No. 158. Thus, the question is whether the remaining Plaintiffs adequately allege that Zoom disclosed their device data through Facebook's SDK. The answer is no. Plaintiffs instead suggest that they used app versions that either (1) had removed Facebook's SDK; or (2) were not iOS apps. As to the removal of Facebook's SDK, some Plaintiffs allege only that they used Zoom on an iPhone *after* March 27, 2020. *See, e.g.*, FAC ¶¶ 37 (Heddi Cundle's May 6, 2020 incident), 41 (Oak Life's April 19, 2020 incident), 55 (Peter Hirshberg's May 30, 2020 event). Other Plaintiffs fail to allege when they have used Zoom, let alone Zoom's iOS app. *See, e.g.*, *id.* ¶¶ 19 (Kristen Hartmann), 25 (Lisa T. Johnston), 45 (Stacey Simins alleging she used Zoom on "multiple occasions" at unspecified times). As to non-iOS apps, the only other Plaintiff to allege using Zoom before March 27, 2020—Plaintiff Isabelle Gmerek—does not allege using Zoom on an iPhone. FAC ¶¶ 21, 23.

Thus, since Gormezano's voluntary dismissal, Plaintiffs inadequately allege that Zoom's implementation of Facebook's SDK invaded Plaintiffs' privacy under California law. Adequate allegations would include information "regarding the participants in the conversations, the locations of the conversations, or examples of content from the conversations." *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 817 (N.D. Cal. 2020); *accord, e.g.*, *Banga*, 2015 WL 3799546, at *9 (requiring plaintiff to allege "what particular information was disclosed"); *Low*, 900 F. Supp. 2d at 1025 (same). Indeed, Plaintiffs fail to plausibly allege that the Facebook SDK was even implemented on Plaintiffs' devices.

2. Plaintiffs inadequately allege that Zoom shared their personal data through Zoom's Android app.

Similarly, the other data-sharing claims—claims that Zoom shares Plaintiffs' data through Zoom's Android app and the LinkedIn Sales Navigator—are also foreclosed by their conclusory vagueness. As to data sharing through Zoom's Android app, Plaintiffs candidly admit that not all instances of Zoom's Android app will share user data. Rather, whether Zoom's Android app shares user data "*depend[s] on the smartphone and operating system*." FAC ¶ 110 (emphasis added).

Plaintiffs also cite privacy testing by AppCensus, but fail to note that according to AppCensus, many versions of Zoom's Android app do not appear to share user data. *Compare* FAC ¶¶ 110, 128 (citing AppCensus, *AppSearch: ZOOM Cloud Meetings, Version 4.3.46323* (Jan. 28, 2019), https://search.appcensus.io/app/us.zoom.videomeetings/43002; and *id.* at *Version 4.1.34821* (Nov. 22, 2018), https://search.appcensus.io/app/us.zoom.videomeetings/41020#), *with, e.g.*, AppCensus, *supra*, at *Version 4.4.52582* (Apr. 16, 2019), https://search.appcensus.io/app/us.zoom.videomeetings/44005 (finding no personal data transmitted during testing).

In short, by the FAC's own terms, Zoom's Android app often does *not* transmit user data. Yet Plaintiffs fail to allege that *their* Android devices transmitted personal information. Plaintiffs in fact provide no information about their "smartphone and operating system" or their version(s) of the Zoom Android app. FAC ¶ 110. For instance, Plaintiffs fail to allege (1) the model of Android smartphone(s) Plaintiffs have used over time; (2) the version(s) of the Android operating system on those smartphones over time; (3) the version(s) of the Zoom Android app on those smartphones over time; and (4) whether Plaintiffs' particular combination(s) of smartphone/operating system/app plausibly disclosed Plaintiffs' user data. *See, e.g.*, FAC ¶¶ 21 (Gmerek's "Android phone"), 27 (M.F.'s "Android phone"), 29 (Therese Jimenez's "Android phone"). Thus, Plaintiffs have failed to meet their burden of alleging "what information, precisely, [certain] third parties have obtained." *E.g.*, *Low*, 900 F. Supp. 2d at 1025.

3. Plaintiffs inadequately allege that Zoom shared their personal data through LinkedIn Sales Navigator.

LinkedIn Sales Navigator, for its part, only provides information to unauthorized third parties on three conditions alleged in the FAC. First, a third party must subscribe to LinkedIn Sales Navigator, a service for sales prospecting sold by LinkedIn. FAC ¶ 123. Second, the third party must join a Zoom meeting in which the other participants have not agreed to share their LinkedIn profiles. *Id.* Lastly, the third party must "click on a LinkedIn icon next to" each other participants' name to view that person's LinkedIn data. *Id.*

Plaintiffs fail to allege that any of these conditions have applied to them. That is, the FAC fails to allege that any Plaintiff (1) has reason to believe that Plaintiff was in a meeting with a LinkedIn Sales Navigator subscriber; (2) has a LinkedIn profile, let alone one Plaintiff would like to keep private; and (3) has reason to believe that a LinkedIn Sales Navigator subscriber actually clicked on Plaintiff's name to access Plaintiff's private LinkedIn data. *See* FAC ¶¶ 17–59 (failing to mention LinkedIn). Thus, just as the Court dismissed the *Low* plaintiffs' invasion of privacy claims against LinkedIn because "it [was] not clear . . . what information, precisely, [certain] third parties have obtained," the Court dismisses Plaintiffs' claims here too. *Low*, 900 F. Supp. 2d at 1025.

In sum, Plaintiffs fail to allege that Zoom actually shared *their* personal data with third parties. The Court thus dismisses Plaintiffs' invasion of privacy claim (Count 1). However, the Court allows Plaintiffs leave to amend because amendment would not unduly prejudice the opposing party, cause undue delay, or be futile, and Plaintiffs have not acted in bad faith. *See Leadsinger*, 512 F.3d at 532.

C. Count 2: The economic loss rule bars Plaintiffs' negligence claim.

Count 2 of the FAC alleges that Zoom was negligent. Zoom moves to dismiss this negligence claim on two grounds. Zoom first argues that "[t]he economic loss rule bars Plaintiffs' claim[]." Reply at 6. Zoom next argues that Plaintiffs have failed to plead the elements of negligence. *Id.* at 7. The Court agrees that the economic loss rule bars Plaintiffs' negligence claim. Thus, the Court need not address the elements of negligence.

"Quite simply, the economic loss rule 'prevents the law of contract and the law of tort from dissolving one into the other.'" *Robinson Helicopter Co. v. Dana Corp.*, 102 P.3d 268, 273 (Cal. 2004) (quoting *Rich Products Corp. v. Kemutec, Inc.*, 66 F. Supp. 2d 937, 969 (E.D. Wis. 1999)). "Under the economic loss rule, 'purely economic losses are not recoverable in tort.'" *R Power Biofuels, LLC v. Chemex LLC*, No. 16-CV-00716-LHK, 2016 WL 6663002, at *4 (N.D. Cal. Nov. 11, 2016) (quoting *NuCal Foods, Inc. v. Quality Egg LLC*, 918 F. Supp. 2d 1023, 1028 (E.D. Cal. 2013)). The rule applies unless a plaintiff adequately alleges "(1) personal injury, (2) physical

damage to property, (3) a "special relationship" existing between the parties, or (4) some other common law exception to the rule." *Kalitta Air, L.L.C. v. Cent. Texas Airborne Sys., Inc.*, 315 F. App'x 603, 605 (9th Cir. 2008).

Here, Plaintiffs invoke three exemptions to the economic loss rule: (1) personal injury; (2) a special relationship between Plaintiffs and Zoom; and (3) the "independent duty exception" for tortious breaches of contract. Opp'n at 11. None apply here.

First, Plaintiffs' invocation of the personal injury exception is a "bare assertion in a brief with no supporting argument." *E.g.*, *Parrish v. Mabus*, 679 F. App'x 620, 621 (9th Cir. 2017). Plaintiffs devote just one sentence to the exception: "Plaintiffs also allege mental suffering (*i.e.*, personal injury) from Zoom's failure to preclude Zoombombers." Opp'n at 12. This short sentence is devoid of any legal authority. Thus, the Court finds that the personal injury exception does not apply.

Second, Plaintiffs and Zoom lack a "special relationship." To reach this conclusion, the court weighs "'the sum total' of the policy considerations at play," guided by "the need to safeguard the efficacy of tort law by setting meaningful limits on liability." *S. California Gas Leak Cases*, 441 P.3d 881, 887 (2019) (quoting *Bily v. Arthur Young & Co.*, 834 P.2d 745, 761 (Cal. 1992), *as modified* (Nov. 12, 1992)). Six factors inform the Court's balancing of "the policy considerations at play":

> (i) "the extent to which the transaction was intended to affect the plaintiff," . . . (ii) "the foreseeability of harm to the plaintiff," (iii) "the degree of certainty that the plaintiff suffered injury," (iv) "the closeness of the connection between the defendant's conduct and the injury suffered," (v) "the moral blame attached to the defendant's conduct," and (vi) "the policy of preventing future harm."

Id. (quoting *J'Aire Corp. v. Gregory*, 598 P.2d 60, 63 (Cal. 1979)). All these factors show that Plaintiffs and Zoom lack a special relationship.

The first factor asks whether "the product manufacturer had [] specially made the [product] for the benefit of" Plaintiffs. *Greystone Homes, Inc. v. Midtec, Inc.*, 168 Cal. App. 4th 1194, 1231 (2008) (collecting cases). Where Plaintiffs "were no different from any other purchaser of the

same product," no special relationship exists. *Id.*; *accord In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 969 (S.D. Cal. 2014) (rejecting special relationship based on "everyday consumer transactions"). Here, Plaintiffs are among "millions of consumers[]" who use Zoom and have been affected by Zoom's alleged failures. FAC ¶ 146. Thus, contrary to the first factor, Zoom did not "specially ma[ke]" its video conferencing platform "for the benefit of" Plaintiffs. *Greystone Homes*, 168 Cal. App. 4th at 1231.

The second, third, fourth, and fifth factors also weigh against Plaintiffs. Plaintiffs fail to allege whether *their* information was "compromised or obtained by third parties without consent." *See* Section III-B-1, *supra* (analyzing each Plaintiffs' allegations). As for Plaintiffs' injuries from third parties' Zoombombing, § 230 largely forecloses Zoom's liability for those third-party intrusions. *See* Section III-A, *supra*. Thus, based on the FAC, the second through fifth factors weigh against Plaintiffs.

The sixth factor also fails to support a special relationship. On the record and briefs here, holding Zoom liable would not necessarily further a "policy of preventing future harm." *J'Aire Corp.*, 598 P.2d at 63. Like the retailer-defendant in *Mega RV*, Zoom has incentives to maintain its reputation and relationship with consumers. *Mega RV*, 225 Cal. App. 4th at 1342. Indeed, in the only case Plaintiffs cite to support the sixth factor, "[t]he economic loss rule [was] [] *irrelevant*." *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 799 n.20 (N.D. Cal. 2019) (emphasis added); *see* Opp'n at 14 (citing *In re Facebook*).

Given these factors, the Court follows the California Supreme Court's admonition to "safeguard the efficacy of tort law by setting meaningful limits on liability." *S. California Gas Leak Cases*, 441 P.3d at 887. Plaintiffs have not shown a special relationship between them and Zoom.

Lastly, Plaintiffs invoke the independent duty exception. "The independent duty exception to the economic loss rule applies where the defendant's conduct 'violates a duty independent of the contract arising from principles of tort law.'" *R Power Biofuels*, 2016 WL 6663002, at *10 (quoting *Erlich v. Menezes*, 981 P.2d 978, 983 (Cal. 1999)). As Zoom correctly notes, the

independent duty exception is plainly inapposite here. As the California Supreme Court has explained, the exception "focus[es] on intentional conduct." *Robinson Helicopter*, 102 P.3d at 274. Otherwise, contractual limitations on liability would be "meaningless, as would the statutory distinction between tort and contract remedies." *Id.* (quoting *Erlich*, 981 P.2d at 985). Here, Plaintiffs do not plead intentional misconduct. Thus, the independent duty exception fails to apply.

Accordingly, the Court dismisses Plaintiffs' negligence claim. However, the Court allows Plaintiffs leave to amend because amendment would not unduly prejudice the opposing party, cause undue delay, or be futile, and Plaintiffs have not acted in bad faith. *See Leadsinger*, 512 F.3d at 532.

D. Count 3: Because Zoom has not shown that Plaintiffs agreed to Zoom's terms of service, Plaintiffs adequately plead a violation of implied contract.

Count 3 alleges that Plaintiffs and Zoom "entered into implied contracts, separate and apart from Zoom's terms of service, under which Defendant agreed to and was obligated to take reasonable steps to secure and safeguard [Plaintiffs'] sensitive information." FAC ¶ 228. Zoom argues that, except for minor Plaintiff M.F., "Plaintiffs may not maintain an implied contract claim because an express written agreement—Zoom's terms of service ('TOS')—controls." Mot. at 17. Zoom's argument rests on the rule that "[t]here[] cannot be a valid, express contract and an implied contract, each embracing the same subject matter, existing at the same time." *Allied Trend Int'l, Ltd. v. Parcel Pending, Inc.*, No. 2019 WL 2150404, at *3 (C.D. Cal. Mar. 25, 2019) (quoting *Wal-Noon Corp. v. Hill*, 45 Cal. App. 3d 605, 613 (1975)).

Plaintiffs respond to Zoom's TOS argument in three ways. First, Plaintiffs allege that their data is shared with Facebook even before they see the TOS. Specifically, Plaintiffs allege that "for every app implementing the Facebook SDK," such as certain versions of Zoom's iOS app, "Facebook starts receiving data on its servers the second the installation process begins," FAC ¶ 85; *see* Opp'n at 18 (citing FAC ¶ 85). Second, Plaintiffs respond that the TOS's mere existence fails to show that Plaintiffs and Zoom had an express contract. To show an express contract, Plaintiffs reason, Zoom would have to prove that a "reasonably prudent" user would have been

"on inquiry notice of the terms of the [TOS]." *Id.* at 17 (quoting *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014)). Third, Plaintiffs respond that even if the TOS bound Plaintiffs, the TOS fails to apply to Plaintiffs' implied contract because the TOS concerns different subject matter. *Id.* at 18.

The Court analyzes Plaintiffs' first two responses below. Because the Court finds Plaintiffs' second response dispositive, the Court need not analyze Plaintiffs' third response.

1. Plaintiffs inadequately allege that the Zoom app must have sent Plaintiffs' data to third parties before Plaintiffs registered for a Zoom account.

Plaintiffs' first response is ultimately unpersuasive even though its premise is sound. The response's premise is that "every app implementing the Facebook SDK" sends device data to Facebook "the second the [app's] installation process begins." FAC ¶ 85. For Zoom's app, the installation process would occur "before the user would have even encountered Zoom's terms and conditions or any privacy disclosures." *Id.* It is undisputed that a user only encounters (and agrees) to Zoom's TOS upon registering an account. *See, e.g.*, Opp'n at 17–18; Reply at 10.

Thus, by the FAC's own terms, for Zoom to send a Plaintiff's information to Facebook before that Plaintiff agrees to Zoom's TOS, two things must be true. To start, a Plaintiff must have installed a version of the Zoom app *that implemented Facebook's SDK*. Plaintiff then must have installed that version of Zoom *before* having registered an account on another device.

The FAC fails to allege that any Plaintiff meets both conditions. As detailed in Section III-A-1 *supra*, only former Plaintiff Cynthia Gormezano plausibly alleges that she ever used a version of the Zoom app that implemented Facebook's SDK (*i.e.*, a pre-March 27, 2020 version of the iOS app). Current Plaintiffs instead suggest that they started using Zoom only after Zoom had updated its iOS app to remove Facebook's SDK. *See* Section III-A-1, *supra*. As for Gormezano, even she fails to allege that she installed the iOS app before registering a Zoom account. *See* FAC ¶¶ 50–52 (Gormezano's allegations). To the contrary, because Gormezano also accessed Zoom through her Windows laptop, Gormezano may have used that laptop to register a Zoom account before she started using Zoom on her iPhone. FAC ¶ 50.

Accordingly, the FAC fails to adequately allege that Zoom shares any Plaintiff's information with Facebook before that Plaintiff agrees to Zoom's TOS.

2. Zoom fails to show that Plaintiffs and Zoom had an express contract.

By contrast, Plaintiffs' second response to Zoom's TOS argument *does* support Plaintiffs' implied contract claim. Plaintiffs argue that the TOS's mere existence fails to show that Plaintiffs and Zoom had an express contract. Plaintiffs offer two reasons why. First, Plaintiffs argue that, on a motion to dismiss, Zoom's declaration is not evidence that Plaintiffs agreed to the TOS. Opp'n at 17. Second, Plaintiffs argue that even if the Court were to credit Zoom's declaration, the declaration is too conclusory to show that "a reasonably prudent user" would be on notice of the TOS—a requirement for the TOS's validity. *Id.* (quoting *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014)).

Both of Plaintiffs' reasons are persuasive. First, the Court cannot consider Zoom's declaration on a motion to dismiss. On a Rule 12(b)(6) motion to dismiss, the Court cannot consider evidence outside the pleadings—such as Zoom's declaration—without (1) "convert[ing] the 12(b)(6) motion into a Rule 56 motion for summary judgment"; and (2) "giv[ing] the nonmoving party an opportunity to respond." *United States v. Ritchie*, 342 F.3d 903, 907 (9th Cir. 2003). Zoom does not ask the Court to do either of these things.

Second, even if the Court were to credit Zoom's declaration on a motion to dismiss, the declaration is too conclusory to show that Zoom's TOS constitute an express contract. "[W]here, as here, there is no evidence that the [Zoom] user had actual knowledge of the [TOS]," whether the TOS constitute an express contract turns on whether Zoom "put[] a reasonably prudent user on inquiry notice of the [TOS]." *Nguyen*, 763 F.3d at 1177. Zoom's declaration fails to prove inquiry notice in two respects.

For one, it is unclear whether declarant Jacqueline Hill—a paralegal for Zoom—has personal knowledge that each Plaintiff encountered the TOS upon registering for a Zoom account. *See* Jacqueline Hill Decl. ¶¶ 1–2, ECF No. 121-1 (providing Hill's job title and extent of knowledge). "Declarations must be made with personal knowledge; declarations not based on

personal knowledge are inadmissible and cannot raise a genuine issue of material fact." *Hexcel Corp. v. Ineos Polymers, Inc.*, 681 F.3d 1055, 1063 (9th Cir. 2012). Rather than assert personal knowledge, Hill vaguely states that her declaration is based *either* on her personal knowledge "or upon [her] review of the business records of Zoom, or from information transmitted by a person with knowledge of the facts described herein." *Id.* ¶ 2.

For another, Zoom's declaration "lack[s] detailed facts and any supporting evidence." *Hexcel Corp.*, 681 F.3d at 1063 (quoting *FTC v. Publ'g Clearing House, Inc.*, 104 F.3d 1168, 1171 (9th Cir. 1997)). The declaration asserts, in one short paragraph without supporting screenshots, that "[w]henever an individual chooses to register for a Zoom account, they are presented with the Terms of Service on their device and asked to click 'Confirm.'" Hill Decl. ¶ 4. The entirety of this self-serving paragraph is as follows:

> Whenever an individual chooses to register for a Zoom account, they are presented with the Terms of Service on their device and asked to click "Confirm." On that same screen, a potential registrant is also informed that: "By signing up, I agree to the Privacy Policy and Terms of Service." An individual cannot register for an account without clicking "Confirm," thereby agreeing to the Terms of Service.

Id. ¶ 4. As analyzed below, this conclusory paragraph lacks facts showing that each Plaintiff had "inquiry notice of the [TOS]." *Nguyen*, 763 F.3d at 1177.

For example, the declaration lacks facts to show whether the TOS were presented to each Plaintiff in a conspicuous way. As then-Circuit Judge Sotomayor explained, "California's common law is clear that 'an offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious.'" *Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17, 30 (2d Cir. 2002) (Sotomayor, J.) (quoting *Windsor Mills, Inc. v. Collins & Aikman Corp.*, 101 Cal. Rptr. 347, 351 (Ct. App. 1972)). The conspicuousness of the TOS would turn on details such as whether (1) the TOS were (i) displayed in full, (ii) hyperlinked, or (iii) simply mentioned without explanation; (2) font size and color; and (3) the distance between the statement "I agree to the Privacy Policy and the Terms of Service" and the "Confirm" button. *See generally Nguyen*, 763 F.3d at 1176–77

(citing cases analyzing whether terms of service were conspicuous). None of this information is in Zoom's conclusory declaration.

Furthermore, what information each Plaintiff saw may have varied by each Plaintiff. Each Plaintiff has accessed Zoom at different times and on different devices. *See* Section I-A, *supra* (detailing each Plaintiff's devices and specific Zoom incidents alleged in FAC). Zoom's declaration does not aver that Zoom presents its TOS in the same manner on all relevant devices at all relevant times.

In sum, on this motion to dismiss, Zoom lacks support for its assertion that all Plaintiffs except M.F. agreed to Zoom's TOS. Accordingly, the Court denies Zoom's motion to dismiss Plaintiffs' implied contract claim.

E. Count 4: Plaintiffs adequately allege that Zoom breached the implied covenant of good faith and fair dealing.

Count 4 of the FAC alleges that Zoom breached the implied covenant of good faith and fair dealing. Zoom's only argument against this claim is that it duplicates the implied contract claim. Mot. at 18–19; Reply at 11. In Zoom's view, both claims should rise or fall together.

As explained in the previous Section, the implied contract claim survives Zoom's motion to dismiss. Accordingly, Plaintiffs' implied covenant claim also survives.

F. Count 8: Plaintiffs inadequately allege harm under California's Comprehensive Data Access and Fraud Act ("CDAFA").

Count 8 of the FAC alleges that Zoom has violated seven provisions of California's Comprehensive Data Access and Fraud Act ("CDAFA"), California Penal Code § 502. CDAFA is an anti-hacking statute intended to protect Californians' "computers, computer systems, and data." Cal. Penal Code § 502(a). The seven provisions that Zoom allegedly violated are California Penal Code §§ 502(c)(1)(B), (c)(2), (c)(3), (c)(6), (c)(7), (c)(8), and (c)(13). These provisions of § 502(c) impose liability on any person who commits enumerated acts related to obtaining Plaintiffs' data.[3]

[3] Specifically, the seven provisions hold liable any person who:

However, for a plaintiff to have a private cause of action under these provisions, that plaintiff must have "suffer[ed] damage or loss." Cal. Penal Code § 502(e)(1).

Zoom moves to dismiss all of Plaintiffs' CDAFA claims on three grounds. First, Zoom argues that "the FAC fails adequately to allege the requisite harm for each claimed violation because, as discussed above, . . . Plaintiffs have not alleged that Zoom disclosed any of *their* personal information." Mot. at 19. Second, Zoom argues that Plaintiffs' allegations are too conclusory because they "merely track[] the language of the statute itself, without providing facts to substantiate the claimed legal conclusions." *Id.* (quoting *Ticketmaster L.L.C. v. Prestige Ent. W., Inc.*, 315 F. Supp. 3d 1147, 1175 (C.D. Cal. 2018)). Third, Zoom argues that because Plaintiffs "voluntarily installed Zoom's software and used its services," none of Plaintiffs' CDAFA claims

---

> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to . . . (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> (3) Knowingly and without permission uses or causes to be used computer services. . . .
>
> (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
>
> (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network. . . .
>
> (13) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section.

Cal. Penal Code §§ 502(c).

can proceed. *Id.* at 20.

The Court agrees with Zoom's first argument. As explained below, Plaintiffs have inadequately alleged harm to support a CDAFA cause of action. Because this conclusion requires dismissal of Plaintiffs' CDAFA claims, the Court need not reach Zoom's other arguments.

To bring a CDAFA claim, a private owner of data must adequately allege that she "suffer[ed] *damage or loss* by reason of a violation of" CDAFA. Cal. Penal Code § 502(e)(1) (emphasis added). Zoom argues that Plaintiffs have failed to adequately allege "damage or loss" because "Plaintiffs have not alleged that Zoom disclosed any of *their* personal information." Mot. at 19. Plaintiffs respond that the Ninth Circuit's decision in "*Facebook Internet Tracking* dispenses with Zoom's argument that Plaintiffs somehow fail to allege the requisite 'damage or loss.'" Mot. at 19 (citing 956 F.3d at 600).

The Court agrees with Zoom. Plaintiffs have inadequately alleged damage or loss. As the Court explained in Section III-B, *supra*, only former Plaintiff Cynthia Gormezano may have adequately alleged that Zoom disclosed her data to third parties. Other Plaintiffs fail to allege facts that plausibly show that *Plaintiffs*' private data was disclosed, such as facts "regarding the participants in the conversations, the locations of the conversations, or examples of content from the conversations" in which Plaintiffs' private data was disclosed. *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 817; *accord, e.g.*, *Banga*, 2015 WL 3799546, at *9 (requiring plaintiff to allege "what particular information was disclosed"); *Low*, 900 F. Supp. 2d at 1025 (requiring same). As it stands, the FAC merely alleges that Zoom has disclosed certain other people's data, not necessarily *Plaintiffs*' data.

Thus, the remaining question is whether Plaintiffs are right that *Facebook Internet Tracking* nonetheless holds that Plaintiffs' allegations are sufficient. The answer is no. *Facebook Internet Tracking* is inapposite. There, unlike here, the parties agreed that Facebook gathered plaintiffs' data. Facebook "track[ed] users' browsing histories when they visit third-party websites"—even after users had logged out of Facebook—"and then compile[d] these browsing histories into personal profiles which are sold to advertisers to generate revenue." *Facebook*

Internet Tracking, 956 F.3d at 596. Despite conceding that it gathered plaintiffs' data, Facebook argued that its "unjustly earned profits" from plaintiffs' data was not enough for Article III standing. *Id.* at 600. The Ninth Circuit disagreed. *Id.* at 601.

Here, Zoom successfully disputes whether Zoom shared Plaintiffs' data with third parties. It is unclear if Zoom has shared, let alone sold, any of Plaintiffs' data. Thus, Plaintiffs fail to allege that Zoom profited from Plaintiffs' data. In other words, *Facebook Internet Tracking* has nothing to say about the CDAFA claims of plaintiffs who have failed to allege that defendant has (1) unjustly shared their data; and (2) profited from that sharing. *See Facebook Internet Tracking*, 956 F.3d at 600 (discussing *McBride v. Boughton*, 123 Cal. App. 4th 379, 389 (2004)).

Accordingly, the Court dismisses Plaintiffs' CDAFA claims. However, the Court allows Plaintiffs leave to amend because amendment would not unduly prejudice the opposing party, cause undue delay, or be futile, and Plaintiffs have not acted in bad faith. *See Leadsinger*, 512 F.3d at 532.

G. Counts 6, 7, and 9: Plaintiffs inadequately allege claims under the Unfair Competition Law ("UCL"), Consumer Legal Remedies Act ("CLRA"), and California Civil Code § 1710(3) fraudulent concealment.

Counts 6, 7, and 9 of the FAC claim that Zoom violated California's Unfair Competition Law (the "UCL," Cal. Bus. & Prof. Code § 17200, *et seq.*) (Count 6); California's Consumer Legal Remedies Act (the "CLRA," Cal. Civ. Code § 1750, *et seq.*) (Count 7); and California Civil Code § 1710(3)'s prohibition against deceit by concealment (Count 9). The parties analyze these claims together for the purposes of the instant motion.

Zoom moves to dismiss these claims on four grounds. First, Zoom argues that the claims are all fraud-based claims that fail the heightened pleading requirements of Federal Rule of Civil Procedure 9(b). Mot. at 20. Second, Zoom argues that all but four Plaintiffs cannot maintain CLRA claims because they are not "consumers" under the CLRA. *Id.* at 22–23. Third, Zoom argues that the four remaining Plaintiffs' CLRA claims for damages fail because those Plaintiffs did not provide Zoom the required pre-suit notice. *Id.* at 23–24. Lastly, Zoom argues that the Plaintiffs otherwise fail to state a claim under the UCL's "unlawful" and "unfair" prongs. *Id.* at

24–25.

The Court agrees with Zoom's first argument. As explained below, the fraud-based claims fail to satisfy Rule 9(b). Because this conclusion requires dismissal of Plaintiffs' CLRA claim, the Court need not address Zoom's second and third argument. As to Zoom's last argument, however, the Court concludes that Plaintiffs do state a claim under the UCL's unlawful and unfair prongs. Below, the Court first addresses Rule 9(b) and then the UCL's non-fraud prongs.

1. Plaintiffs' fraud-based claims fail to satisfy the heightened pleading requirements of Federal Rule of Civil Procedure 9(b).

Zoom first argues that Counts 6, 7, and 9 are "are all based on Zoom's alleged course of conduct fraudulently 'misrepresent[ing]' or 'omitt[ing]' information about the privacy and security features of its services." Mot. at 20 (alterations in original) (citing FAC ¶¶ 250–278, 293–298). As a result, Zoom argues, the FAC "as a whole must satisfy the particularity requirement of Rule 9(b)." *Id.* (quoting *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009)).

Plaintiffs have two responses. First, Plaintiffs respond that Rule 9(b) does not apply to Plaintiffs' UCL claims of "unlawful" or "unfair" conduct. Opp'n at 20, 23. Second, Plaintiffs argue that their allegations satisfy Rule 9(b) by (1) identifying "affirmative statements by Zoom" that were allegedly fraudulent; and (2) pleading Plaintiffs' reliance on those statements. *Id.* at 20–21.

The Court agrees with Plaintiffs' first response but not Plaintiffs' second. As to the first response, Zoom does not dispute on Reply that Plaintiffs' UCL claims of unlawful or unfair conduct are not subject to Rule 9(b). Instead, Zoom analyzes those claims separately. *See* Reply at 12–13 (analyzing Rule 9(b)), 14–15 (analyzing UCL). This separate analysis is required because "[e]ach prong of the UCL"—proscribing unlawful, unfair, and fraudulent acts— "is a separate and distinct theory of liability." *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). Only claims sounding in fraud are subject to the heightened pleading requirements of Rule 9(b). *Bly-Magee v. California*, 236 F.3d 1014, 1018 (9th Cir. 2001). Thus, the issue is whether Counts 6, 7, and 9's fraud-based claims satisfy Rule 9(b).

Rule 9(b) requires that claims sounding in fraud allege "an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations." *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007). In other words, "[a]verments of fraud must be accompanied by 'the who, what, when, where, and how' of the misconduct charged." *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (quoting *Cooper v. Pickett*, 137 F.3d 616, 627 (9th Cir. 1997)). A plaintiff must also plead facts explaining why the statement was false when it was made. *See In re GlenFed, Inc. Sec. Litig.,* 42 F.3d 1541, 1549 (9th Cir. 1994) (en banc), *superseded by statute on other grounds as stated in Adomitis ex. rel. United States v. San Bernardino Mountains Cmty. Hosp. Dist.*, 816 F. App'x 64, 66 (9th Cir. 2020).

Plaintiffs' fraud-based claims fail to meet Rule 9(b)'s standard. Plaintiffs fail to allege "*who* actually saw *what* misrepresentations/omissions and *when* and *where* they saw" the misrepresentations or omissions. Mot. at 12 (emphasis added); *accord Vess*, 317 F.3d at 1106. Rather, Plaintiffs merely "identify[] the statements on Zoom's website and privacy policy that are reasonably likely to mislead." Opp'n at 20 (citing FAC ¶¶ 129–39, 163–66). No Plaintiff alleges reading those allegedly misleading statements, let alone reading them at a specific time or place. *See* FAC ¶¶ 17–59 (each Plaintiff's allegations). This proves fatal for Plaintiffs' fraud-based claims. *See, e.g.*, *Phillips v. Apple Inc.*, No. 15-CV-04879-LHK, 2016 WL 1579693, at *8 (N.D. Cal. Apr. 19, 2016) (dismissing UCL claims for plaintiffs' failure to "plead that they viewed or heard any representations or omissions"; and collecting cases); *Davidson v. Apple, Inc.*, No. 16-CV-04942-LHK, 2017 WL 976048, at *9–10 (N.D. Cal. Mar. 14, 2017) (dismissing fraudulent omissions claims on similar grounds).

Davidson v. Apple is an especially instructive example. There, the Court disapproved of the fact that "for some [p]laintiffs, the [complaint] does not even provide the date on which the [p]laintiff made his or her purchase." *Davidson*, 2017 WL 976048, at *10. Here, the FAC is even more flawed. It fails to provide *any* Plaintiff's date of purchase—or any other date on which any Plaintiff would have seen Zoom's alleged misrepresentations about privacy. *See* FAC ¶¶ 17–59

(each Plaintiff's allegations).

In response, Plaintiffs rely on *Ehret v. Uber Techs., Inc.*, 68 F. Supp. 3d 1121, 1129 (N.D. Cal. 2014). Yet *Ehret* actually supports Zoom's position. The *Ehret* plaintiff satisfied Rule 9(b) by alleging (1) the date she used Uber; (2) alleged misrepresentation she saw on that date; and (3) where Uber made that alleged misrepresentation. *Id.* Specifically, the *Ehret* plaintiff alleged that on September 9, 2012 in Chicago, Uber's smartphone application misrepresented to her that a 20% surcharge was a "gratuity" for her driver. *Id.* at 1127, 1129. Here, by contrast, Plaintiffs fail to allege when and where they saw all (or even some) of the many misrepresentations alleged in FAC ¶¶ 250–278 and ¶¶ 293–298.

Accordingly, the Court dismisses Count 6's claim of fraudulent conduct; Count 7; and Count 9. However, the Court allows Plaintiffs leave to amend because amendment would not unduly prejudice the opposing party, cause undue delay, or be futile, and Plaintiffs have not acted in bad faith. *See Leadsinger*, 512 F.3d at 532.

2. Plaintiffs adequately pleads UCL claims under the UCL's "unlawful" and "unfair" prongs.

Count 6 of the FAC brings UCL claims under all three prongs of the UCL. Zoom successfully moves to dismiss the "fraudulent" prong claim under Rule 9(b)'s particularity requirement, as explained just above. *See* Section III-G-1, *supra*. Zoom also moves to dismiss Plaintiffs' claims under the "unlawful" and "unfair" prongs. Zoom first argues that because all of Plaintiffs' other claims fail, "[n]o predicate violation supports Plaintiff[s]' 'unlawful' prong UCL claim." Mot. at 24. Zoom further argues that Plaintiffs' unfair prong claim is conclusory because the claim is untethered to "any specific public policy" or moral principles. *Id.* at 25.

The Court analyzes the unlawful and unfair prongs in turn. "The unlawful prong of the UCL prohibits 'anything that can properly be called a business practice and that at the same time is forbidden by law.'" *Herskowitz v. Apple Inc.*, 940 F. Supp. 2d 1131, 1145 (N.D. Cal. 2013) (quoting *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 973 P.2d 527, 539 (Cal. 1999)). Here, contrary to Zoom's argument, a predicate violation of law supports Plaintiffs' claim.

Plaintiffs adequately allege that Zoom has violated an implied contract with Plaintiffs. *See* Section III-D, *supra* (analyzing implied contract claim, a.k.a. Count 3). Thus, Plaintiffs may maintain their UCL claim under the unlawful prong.

"The 'unfair' prong of the UCL creates a cause of action for a business practice that is unfair even if not proscribed by some other law." *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1226 (N.D. Cal. 2014) (quoting *Korea Supply Co. v. Lockheed Martin Corp.*, 63 P.3d 937, 943 (Cal. 2003)). "The UCL does not define the term 'unfair.' And the proper definition of 'unfair' conduct against consumers 'is currently in flux' among California courts." *Id.* (original alterations omitted) (quoting *Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012)). Courts have offered three distinct definitions of "unfair" conduct toward consumers:

> (1) whether the challenged conduct is "tethered to any underlying constitutional, statutory or regulatory provision, or that it threatens an incipient violation of an antitrust law, or violates the policy or spirit of an antitrust law,"; (2) whether the practice is "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers,"; or (3) whether the practice's impact on the victim outweighs "the reasons, justifications and motives of the alleged wrongdoer."

Doe v. CVS Pharmacy, Inc., 982 F.3d 1204, 1214–15 (9th Cir. 2020) (citations omitted) (first quoting *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1366 (2010), then quoting *Morgan v. AT&T Wireless Servs., Inc.*, 177 Cal. App. 4th 1235, 1254 (2009)); *see also Nationwide Biweekly Admin., Inc. v. Superior Court of Alameda Cty.*, 462 P.3d 461, 472 & n.10 (Cal. 2020) (collecting cases).

Here, contrary to Zoom's arguments, Plaintiffs adequately plead unfair conduct under at least the first test, which is known as the "tethering" test. Under the tethering test, "Plaintiffs do not need to plead any direct violations of a statute . . . . Instead, Plaintiffs need merely to show that the effects of [Zoom]'s conduct 'are comparable to or the same as a violation of the law, or otherwise significantly threaten or harm competition.'" *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d at 1227 (quoting *Cel-Tech,* 20 Cal. 4th at 187). Plaintiffs make that showing here. Plaintiffs specifically argue that Zoom's conduct has impinged the federal Health Insurance Portability and Accountability Act ("HIPAA"), the Children's Online Privacy Protection Act

("COPPA"), and four California consumer protection statutes. *See, e.g.*, FAC ¶¶ 171 (HIPAA), 184–189 (COPPA). Plaintiffs also specify how Zoom allegedly triggered COPPA: by gathering audio or video of minors without obtaining verifiable parental consent, among other things. *Id.* ¶¶ 186, 189. Thus, Zoom is wrong that "[t]he FAC does not tether Plaintiffs' unfair prong claim to any specific public policy." Mot. at 25.

Indeed, Zoom's cited authority supports Plaintiffs. In *Elias v. Hewlett-Packard Co.*, 903 F. Supp. 2d 843, 858 (N.D. Cal. 2012), plaintiff failed to "reference any established public policy that HP's actions have violated or claim that the conduct is immoral, unethical, oppressive, or unscrupulous." *Id.* Here, by contrast, Plaintiffs reference several public policies and allege that Zoom engaged in "immoral, unethical, oppressive, and unscrupulous activities." FAC ¶ 256.

Accordingly, Plaintiffs' adequately allege unfair conduct under the UCL's tethering test. Because tethering is enough to maintain Plaintiffs' UCL claim under the unfair prong, the Court need not reach the other two tests for unfairness. *See, e.g.*, *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *24 (N.D. Cal. Aug. 30, 2017) (denying motion to dismiss unfair prong claim because, "at a minimum," one test for unfairness was met).

H. Count 5: Plaintffs adequately plead a derivative claim of unjust enrichment/quasi-contract.

Lastly, Count 5 of the FAC alleges that Zoom unjustly enriched itself. Zoom argues that "because Plaintiffs' UCL and CLRA claims must be dismissed, their derivative unjust enrichment allegations must as well." Reply at 15. The premise of Zoom's argument is flawed, however. Plaintiffs' UCL claims under the unlawful and unfair prongs survive Zoom's motion to dismiss. *See* Section III-H, *supra* (analyzing UCL). Thus, Plaintiffs' "derivative" unjust enrichment claim survives as well.

IV. CONCLUSION

For the foregoing reasons, the Court GRANTS IN PART and DENIES IN PART Zoom's motion to dismiss the First Amended Complaint. Specifically, the Court GRANTS the motion to

dismiss the following with leave to amend:

- All "Zoombombing" claims to the extent they (1) challenge the harmfulness of content provided by another; and (2) derive from Zoom's status or conduct as a publisher or speaker of that content.
- Count 1: Invasion of privacy under California Law.
- Count 2: Negligence.
- Count 8: California's Comprehensive Data Access and Fraud Act ("CDAFA").
- Counts 6, 7, and 9: Unfair Competition Law ("UCL") claim under the "fraudulent" prong; Consumer Legal Remedies Act ("CLRA"); and California Civil Code § 1710(3) fraudulent concealment.

The Court DENIES the motion to dismiss the following:

- All "Zoombombing" claims to the extent they do not either (1) challenge the harmfulness of content provided by another; or (2) derive from Zoom's status or conduct as a publisher or speaker of that content.
- Count 3: Implied contract.
- Count 4: Implied covenant of good faith and fair dealing.
- Count 6: UCL claims under the "unlawful" and "unfair" prongs.
- Count 5: Unjust enrichment/quasi contract.

Should Plaintiffs elect to file a second amended complaint curing the deficiencies identified herein, Plaintiffs shall do so within 30 days of the date of this order. Failure to meet the 30 day deadline to file a second amended complaint or failure to cure the deficiencies identified in this order or Zoom's motion to dismiss will result in dismissal of the deficient claims with prejudice. Plaintiffs may not add new causes of action or parties without leave of the Court or stipulation of the parties pursuant to Federal Rule of Civil Procedure 15. Plaintiffs are directed to file a redlined complaint comparing the FAC to any second amended complaint as an attachment to Plaintiffs' second amended complaint.

IT IS SO ORDERED.

Dated: March 11, 2021

Lucy H. Koh

LUCY H. KOH
United States District Judge

United States District Court
Northern District of California