UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ELLIOT LIBMAN, et al.,

Plaintiffs,

v.

APPLE, INC.,

Defendant.

Case No. 22-cv-07069-EJD

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Re: ECF No. 122

Plaintiffs bring this class action against Apple for the alleged improper collection and use of Apple mobile device users' data when they interact with Apple's proprietary applications ("apps")—including the App Store, Apple Music, Apple TV, Books, and Stocks (collectively, "Apple Apps")—on their mobile Apple devices (i.e., iPhone, iPad, or Apple Watch). Consolidated Class Action Complaint ("CAC" or "complaint"), ECF No. 115 ¶¶ 1–6. Plaintiffs allege that Apple misled users that certain settings would restrict Apple's collection, storage, and use of private data, when in fact Apple disregarded these choices and collected, stored, and used the data anyway.

Before the Court is Apple's motion to dismiss Plaintiffs' complaint with prejudice under Federal Rules of Civil Procedure 9(b), 12(b)(1) and 12(b)(6). Motion to Dismiss ("Mot." or "Motion"), ECF No. 122. Having reviewed the parties' papers, and having considered the arguments of counsel, the Court GRANTS IN PART and DENIES IN PART Apple's motion.

I. BACKGROUND

Plaintiffs are Ashley Popa, Bruce Puleo, Barry Robinson, Carlina Green, David Sgro, A.H.

(a minor, with Julie Hodges serving as their guardian ad litem), Dottie Nikolich, Elena Nacarino, Francis Barrott, Katie Alvarez, Jarell Brown, Julia Cima, Elizabeth Kelly, E.M. (a minor, with Daryl Marcott serving as their guardian ad litem), and Quincy Venter ("Plaintiffs") who, on behalf of themselves and all others similarly situated, allege that Apple improperly collects and uses Apple mobile device users' data even when Apple allows them to choose settings that purportedly restricted Apple's collection, storage, and use of such data. CAC ¶ 1.

In Plaintiffs' view, Apple has emphasized its purported commitment to consumer privacy through its aggressive marketing strategies, including an ad campaign that began running in 2019 focused on user privacy protections. *Id.* ¶¶ 32–34. In contradiction of these privacy promises, Plaintiffs allege Apple improperly collects and uses their data when they interact with Apple Apps; Plaintiffs do not challenge any data collected from interactions with non-Apple apps. *Id.* Specifically, Apple allegedly tracks and collects large swaths of personal information from Plaintiffs when they use Apple Apps, including "details about app usage, app browsing communications, personal information, and information relating to the mobile device itself." *Id.* ¶ 4.

Plaintiffs' complaint centers on two settings Plaintiffs allege govern the data collection at issue: the "Allow Apps to Request to Track" setting and the "Share [Device] Analytics" setting. *Id.* ¶¶ 45–46. The "Allow Apps to Request to Track" setting states: "Allow apps to ask to track your activity across other companies' apps and websites. When this is off, all new app tracking requests are automatically denied." When the "Allow Apps to Request to Track" setting is turned off, Plaintiffs allege that Apple promises that Apple Apps cannot "access the system advertising identifier (IDFA), which is often used to track" and are "not permitted to track your activity using other information that identifies you or your device, like your email address." *Id.* ¶ 45. In connection with this setting, Apple promises that it "requires app developers to ask for permission before they track your activity across Apps or websites they don't own." *Id.* ¶ 105. The second setting at issue, the "Share [Device] Analytics" setting, states: "Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Data may include location

information. Analytics uses wireless data." Plaintiffs allege that, by turning off the "Share [Device] Analytics" setting, Apple promised that Plaintiffs could "disable the sharing of Device Analytics altogether." *Id.* ¶ 46. If these two settings were turned off, Plaintiffs assert that Apple promised Plaintiffs that their user data would not be collected. Despite those promises, Apple "continu[ed] to collect user data whenever Plaintiffs and the Class interacted with Apple's Apps, such as the App Store, Apple Music, Apple TV, Books, and Stocks," even when users turned off the two settings. *See, e.g.*, *id.* ¶ 116.

Plaintiffs filed their original complaint on November 10, 2022, bringing claims for unjust enrichment (or alternatively, breach of contract), violation of the California Invasion of Privacy Act, and invasion of privacy under California's constitution. ECF No. 1. Thereafter, the case was related to other cases against Apple. *See* ECF Nos. 26, 35, 38, 40. The case was stayed on February 10, 2023, pending resolution of motions to consolidate and to appoint interim lead counsel. ECF No. 27. On March 24, 2023, the Court granted the parties' stipulation to consolidate. ECF No. 60; *see also* ECF Nos. 86, 96. The Court appointed a Plaintiffs' Steering Committee on July 18, 2023. ECF No. 107.

On October 6, 2023, Plaintiffs filed a consolidated amended complaint individually and on behalf of a class of similarly situated individuals alleging Apple's conduct: (1) breaches express contracts; (2) breaches implied contracts; (3) breaches the implied covenant of good faith and fair dealing; (4) amounts to an invasion of privacy; (5) violates California's Invasion of Privacy Act; (6) violates California's Unfair Competition Law; (7) violates Pennsylvania's Wiretapping and Electronic Surveillance Act; (8) violates New York Gen. Bus. Law § 349; (9) violates New York Gen. Bus. Law § 350; (10) violates New Jersey's Consumer Fraud Act; (11) violates Illinois's Consumer Fraud and Deceptive Business Practices Act; and (12) and unjustly enriches Apple.

Apple brought the present motion to dismiss on December 8, 2023, and the motion is fully briefed. Opposition to Motion to Dismiss ("Opp."), ECF 124; Reply in Support of Motion to Dismiss ("Reply"), ECF No. 126. The Court heard oral argument on the motion on March 21, 2024.

II. LEGAL STANDARDS

Federal Rule of Civil Procedure 8(a) requires a plaintiff to plead each claim with sufficient specificity to "give the defendant fair notice of what the ... claim is and the grounds upon which it rests." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (internal quotations omitted). Although particular detail is not generally necessary, the factual allegations "must be enough to raise a right to relief above the speculative level" such that the claim "is plausible on its face." *Id.* at 555, 570. A complaint which falls short of the Rule 8(a) standard may be dismissed if it fails to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). Dismissal of a claim under Rule 12(b)(6) may be based on a "lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1988) (internal citation omitted); *see Ministerio Roca Solida v. McKelvey*, 820 F.3d 1090, 1096 (9th Cir. 2016).

To contest a plaintiff's showing of subject matter jurisdiction, a defendant may file a Rule 12(b)(1) motion. Fed. R. Civ. P. 12(b)(1). A defendant may challenge jurisdiction "facially" by arguing the complaint "on its face" lacks jurisdiction or "factually" by presenting extrinsic evidence demonstrating the lack of jurisdiction on the facts of the case. *Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004); *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). "In a facial attack, the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction. By contrast, in a factual attack, the challenger disputes the truth of the allegations that, by themselves, would otherwise invoke federal jurisdiction." *Safe Air for Everyone*, 373 F.3d at 1039.

In resolving a factual attack on jurisdiction, the Court may review evidence beyond the complaint without converting the motion to dismiss into a motion for summary judgment. Id. (citing *Savage v. Glendale Union High Sch., Dist. No. 205, Maricopa Cty.*, 343 F.3d 1036, 1039 n.2 (9th Cir. 2003)). While the Court may consider evidence outside of the pleadings to resolve a "factual" Rule 12(b)(1) motion, "a [j]urisdictional finding of genuinely disputed facts is inappropriate when the jurisdictional issue and substantive issues are so intertwined that the

question of jurisdiction is dependent on the resolution of factual issues going to the merits of an action." *Safe Air for Everyone*, 373 F.3d at 1039 n.3 (citing *Sun Valley Gasoline, Inc. v. Ernst Enters., Inc.*, 711 F.2d 138, 140 (9th Cir. 1983)) (internal quotation marks omitted).

Claims that sound in fraud are further subject to a heightened pleading standard. Fed. R. Civ. Proc. 9(b) ("In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake."); *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103–04 (9th Cir. 2003) (recognizing that claims "grounded in fraud" or which "sound in fraud" must meet the Rule 9(b) pleading standard, even if fraud is not an element of the claim). The allegations must be "specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong." *Semegen v. Weidner*, 780 F.2d 727, 731 (9th Cir. 1985). This requires 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) (quoting *Edwards v. Marin Park, Inc.*, 356 F.3d 1058, 1066 (9th Cir. 2004)). In other words, fraud or claims asserting fraudulent conduct must generally contain more specific facts than is necessary to support other causes of action. That said, with respect to omissions-based fraud claims, "the pleading standard is lowered on account of the reduced ability in an omission suit 'to specify the time, place, and specific content, relative to a claim involving affirmative misrepresentations.'" *Barrett v. Apple Inc.*, 2021 WL 827235, at *7 (N.D. Cal. Mar. 4, 2021) (quoting *In re Apple & AT&T Mobility Antitrust Litig.*, 596 F. Supp. 2d 1288, 1310 (N.D. Cal. 2008)).

At the motion to dismiss stage, the Court must read and construe the complaint in the light most favorable to the non-moving party. *Cahill v. Liberty Mut. Ins. Co.*, 80 F.3d 336, 337–38 (9th Cir. 1996). Additionally, the Court must accept as true all "well-pleaded factual allegations." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). However, "courts are not bound to accept as true a legal conclusion couched as a factual allegation." *Twombly*, 550 U.S. at 555. Nor is a complaint sufficient if it merely "tenders naked assertions devoid of further factual enhancement." *Iqbal*,

556 U.S. at 678 (internal quotation marks omitted). "In all cases, evaluating a complaint's plausibility is a 'context-specific' endeavor that requires courts to draw on ... judicial experience and common sense." *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014) (quoting *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011)). When deciding whether to grant a motion to dismiss, the Court generally "may not consider any material beyond the pleadings." *Hal Roach Studios, Inc. v. Richard Feiner & Co.*, 896 F.2d 1542, 1555 n.19 (9th Cir. 1990). However, the Court may consider material submitted as part of the complaint or relied upon in the complaint, and may also consider material subject to judicial notice. *See Lee v. City of Los Angeles*, 250 F.3d 668, 688–89 (9th Cir. 2001); *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1139 (9th Cir. 2003) (holding the court is "not required to accept as true conclusory allegations which are contradicted by documents referred to in the complaint.").

If a motion to dismiss is granted, "leave to amend should be granted 'unless the court determines that the allegation of other facts consistent with the challenged pleading could not possibly cure the deficiency.'" *DeSoto v. Yellow Freight Sys.*, 957 F.2d 655, 658 (9th Cir. 1992) (quoting *Schreiber Distrib. Co. v. Serv-Well Furniture Co.*, 806 F.2d 1393, 1401 (9th Cir. 1986)). Leave to amend may also be denied 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. *See Leadsinger, Inc. v. BMG Music Publ'g*, 512 F.3d 522, 532 (9th Cir. 2008).

III. REQUEST FOR JUDICIAL NOTICE

Apple has submitted eighteen exhibits that it asks the Court to review in ruling on its motion to dismiss. Apple's Request for Judicial Notice ("RJN"), ECF 123; *id.* at Exs. 1–18. Apple argues these exhibits are either incorporated by reference by the complaint or subject to judicial notice. Plaintiffs oppose Apple's request. *See* ECF No. 125.

There are two doctrines that permit district courts to consider material outside the pleadings without converting a motion to dismiss into a motion for summary judgment: judicial notice under Federal Rule of Evidence 201 and incorporation by reference. *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 998 (9th Cir. 2018). The judicial notice doctrine permits a court

to take judicial notice of matters that are "not subject to reasonable dispute." Fed. R. Evid. 201(b). A fact is "not subject to reasonable dispute" if it is "generally known," or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b)(1)–(2). However, "[j]ust because the document itself is susceptible to judicial notice does not mean that every assertion of fact within that document is judicially noticeable for its truth." *Khoja*, 899 F.3d at 999. For instance, though public records are generally subject to judicial notice, a court may not take judicial notice of disputed facts within public records. *Id.*

"[I]ncorporation-by-reference is a judicially created doctrine that treats certain documents as though they are part of the complaint itself." *Khoja*, 899 F.3d at 1002. This doctrine permits a court to consider a document "if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim." *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003). A court generally "may assume an incorporated document's contents are true for purposes of a motion to dismiss under Rule 12(b)(6)." *Khoja*, 899 F.3d at 1003 (internal quotations omitted). Because all inferences must still be drawn in the nonmoving party's favor, however, "it is improper to assume the truth of an incorporated document if such assumptions only serve to dispute facts stated in a well-pleaded complaint." *Id.*

Having reviewed the basic principles of judicial notice and incorporation by reference, the Court turns to each of the documents Apple has submitted.

A. Exhibits 1–3

Exhibits 1 and 2 are the iOS and iPadOS 16 Software License Agreement and watchOS 9 Software License Agreement, which govern use of certain technology Plaintiffs claim to have used. Exhibit 3 is a copy of the Privacy Policy referred to in the complaint. These documents "form the basis" for Plaintiffs' claims for breach of contract, implied contract, and implied covenant of good faith and fair dealing claims, as they contain the contract terms that were allegedly breached. *See* CAC ¶¶ 103–14, 122–24, 134. Apple's request to incorporate by reference the software license agreements and Privacy Policy is therefore GRANTED. *See Ritchie*, 342 F.3d at 908.

B. Exhibits 4–8

Exhibits 4–8 are copies of the "welcome screen" that are shown the first time a user opens the Apple Apps at issue in this case. *See* Ex. 4 (welcome screen for App Store); Ex. 5 (welcome screen for Apple Music); Ex. 6 (welcome screen for Apple TV); Ex. 7 (welcome screen for Books); Ex. 8 (welcome screen for Stocks). Apple states that these welcome screens reflect Apple's representations about its privacy practices and privacy settings, which are "integral to plaintiffs' claims and are incorporated by reference." RJN 3.

Although Exhibits 4–8 are not referred to extensively in the complaint, the Court finds they are appropriately incorporated by reference because the welcome screens form the basis Plaintiffs' claim. *Ritchie*, 342 F.3d at 908. Plaintiffs' claims each relate to whether Apple disclosed its collection practices and whether Plaintiffs consented to those collection practices. *See, e.g.*, CAC ¶¶ 110 ("[d]espite promising Plaintiffs and the Class that their user data would not be collected…"), 122 (referring to Apple's "disclosures" which created an implied contract "that Apple would not collect and store user data" under certain circumstances).

Apple's request to incorporate by reference the welcome screens is therefore GRANTED.

C. Exhibits 9–14, 18

Exhibits 9–14 and 18 are copies of various Apple privacy disclosures. *See* Ex. 9 (App Store & Privacy disclosure), Ex. 10 (Apple Music & Privacy disclosure), Ex. 11 (Apple TV App & Privacy disclosure), Ex. 12 (Apple Books & Privacy disclosure), Ex. 13 (Stocks & Privacy disclosure), Ex. 14 (Device Analytics & Privacy disclosure), Ex. 18 (Family Privacy Disclosure for Children).

The various Apple privacy disclosures are available on public websites. *See Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1068 n.3 (N.D. Cal. 2016) (judicially noticing "the Yelp Privacy Policies during the relevant time periods because they were publicly available on the Yelp website"); *see also In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1025, 1028–29 (N.D. Cal. 2014) (judicially noticing Yahoo's Terms of Service ansd Privacy Policy "because they are aspects of a publicly accessible website"). Apple's request that the Court judicially notice the privacy

disclosures is therefore GRANTED.

D. Exhibits 15–17

Finally, Exhibits 15–17 are copies of certain setting screens. Ex. 15 (Share [Device] Analytics setting), Ex. 16 (Allow Apps to Request to Track setting), Ex. 17 (tracking setting disclosure). As with Exhibits 4–8, the Court finds that these Exhibits form the basis of Plaintiffs' claims because the Exhibits reflect the settings Plaintiffs contend they adjusted to protect their privacy. *See, e.g.*, CAC ¶ 44.

Apple's request to incorporate by reference the setting screens is therefore GRANTED.

IV. DISCUSSION

Plaintiffs bring twelve counts against Apple for (1) breach of contract; (2) breach of implied contract; (3) breach of the implied covenant of good faith and fair dealing; (4) invasion of privacy under California's Constitution; (5) violation of California's Invasion of Privacy Act ("CIPA"); (6) violation of California's Unfair Competition Law ("UCL"); (7) violation of Pennsylvania's Wiretapping and Electronic Surveillance Act ("WESCA"); (8) violations of New York Gen. Bus. Law ("GBL") § 349; (9) violation of New York GBL § 350; (10) violation of New Jersey's Consumer Fraud Act ("NJCFA"); (11) violations of Illinois's Consumer Fraud and Deceptive Business Practices Act ("ICFDA"); and (12) unjust enrichment.

Apple moves to dismiss the complaint on several grounds. First, Apple raises two threshold arguments: that Plaintiffs' failure to allege facts about their own experiences warrants dismissal for lack of Article III standing and failure to state a claim, and Plaintiffs' consent to the data collection defeats their claims. Second, Apple contends that Plaintiffs' contract claims are deficient because Plaintiffs cannot establish any breach and have not plausibly plead damages. Third, Apple argues that the complaint does not plausibly allege a wiretap or privacy claim. Fourth, Apple moves to dismiss Plaintiffs' state-law consumer protection claims because Plaintiffs have not adequately alleged a fraudulent statement or deceptive act. Finally, Apple argues that the Court lacks equitable jurisdiction to hear the UCL and unjust enrichment claims. The Court addresses each ground in turn below.

A. Threshold Arguments

1. Standing

Apple first argues that Plaintiffs' claims should be dismissed for lack of Article III standing and under Rule 12(b)(6) because Plaintiffs have not alleged what data was collected from them or any facts about the collection practices of apps beyond those in Plaintiffs' class definition. Mot. 7–9. Apple also contends that the minor Plaintiffs do not allege what apps they used. *Id.* at 8. Plaintiffs respond that *Jones v. Ford Motor Co.*, 85 F.4th 570 (9th Cir. 2023) disposes of Apple's argument. Opp. 4. In that decision, the Ninth Circuit found that plaintiffs who brought claims under the Washington Privacy Act had alleged Article III standing where the operative class action complaint included allegations that Ford vehicles' system "downloads all text messages and call logs from Plaintiffs' cellphones as soon as they are connected," and "the infotainment system permanently stores the private communications without Plaintiffs' knowledge or consent." *Id.* at 574. These allegations, the court found, "plausibly articulate an Article III injury because they claim violation of a substantive privacy right." *Id.* (explaining that "[a] statute that codifies a common law privacy right gives rise to a concrete injury sufficient to confer standing") (quotations omitted).

So too here. The complaint includes allegations that Apple violated a substantive privacy right, including California's Invasion of Privacy Act. Plaintiffs allege that Apple "accessed and recorded" Plaintiffs' data while they were using certain apps, and Plaintiffs "never consented to Apple tracking [their] data while" certain settings were turned off. *See, e.g.*, CAC ¶ 11. At this stage, as in *Jones*, the allegations plausibly articulate an Article III injury because they claim violation of a substantive privacy right.

Apple further argues that even if Plaintiffs have Article III standing, the complaint should nevertheless be dismissed for failure to state a claim because the complaint lacks factual allegations about what data was collected from Plaintiffs. The Court declines to find that, as a threshold matter and without evaluating the pleading requirements for each claim, Plaintiffs' claims are insufficient to state a claim under Rule 12(b)(6). Indeed, the cases Apple relies on to

seek a complaint-wide dismissal made no blanket ruling but rather considered the requirements of each claim. Mot. 8–9; *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d 797, 810–11, 817 (N.D. Cal. 2020) (evaluating counts separately); *see also In re Google Location Hist. Litig.*, 428 F. Supp. 3d 185, 199 (N.D. Cal. 2019) (same). Given the differing legal requirements for each claim, the Court will consider the sufficiency of Plaintiffs' allegations as to each set of claims as opposed to on a complaint-wide basis.

2. Consent

In its next threshold argument for dismissing the complaint, Apple contends that Plaintiffs agreed to the collection of any Apple App data collections through Apple's Privacy Policy, which defeats all claims. Mot. 9–10.

Consent is a defense to Plaintiffs' claims.[1] *See Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 26 (1994) (plaintiff "must not have manifested by his or her conduct a voluntary consent" to alleged privacy violation); *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954 (N.D. Cal. 2017), *aff'd* 745 F. App'x 8 (9th Cir. 2018) (plaintiffs' consent barred CIPA, privacy, and implied covenant claims); *Silver v. Stripe, Inc.*, 2021 WL 3191752, at *4–5 (N.D. Cal. July 28, 2021) (user consent is defense under CIPA); *Hicks v. PGA Tour, Inc.*, 897 F.3d 1109, 1120 n.6 (9th Cir. 2018) (affirming dismissal of unjust enrichment claim based on consent); *Hassler v. Sovereign Bank*, 374 F. App'x 341, 344 (3d Cir. 2010) (NJCFA claim failed where account agreement "clearly explained" the challenged actions); 18 Pa. C.S. § 5704(4) (WESCA permits collection with the parties' "prior consent"); *Chen v. Dunkin' Brands, Inc.*, 954 F.3d 492, 501 (2d Cir. 2020) (explaining that "there can be no [GBL] claim when the allegedly deceptive practice was fully disclosed").

By assenting to the software license agreement, which incorporates Apple's Privacy Policy, and then proceeding to use Apple Apps, Apple argues Plaintiffs consented to the data

[1] Apple has not identified authority showing that consent is a defense to Plaintiffs' ICFDA claims. Accordingly, any ruling as to consent will not apply to Plaintiffs' ICFDA claim. Apple may raise the issue in a future motion to dismiss where applicable.

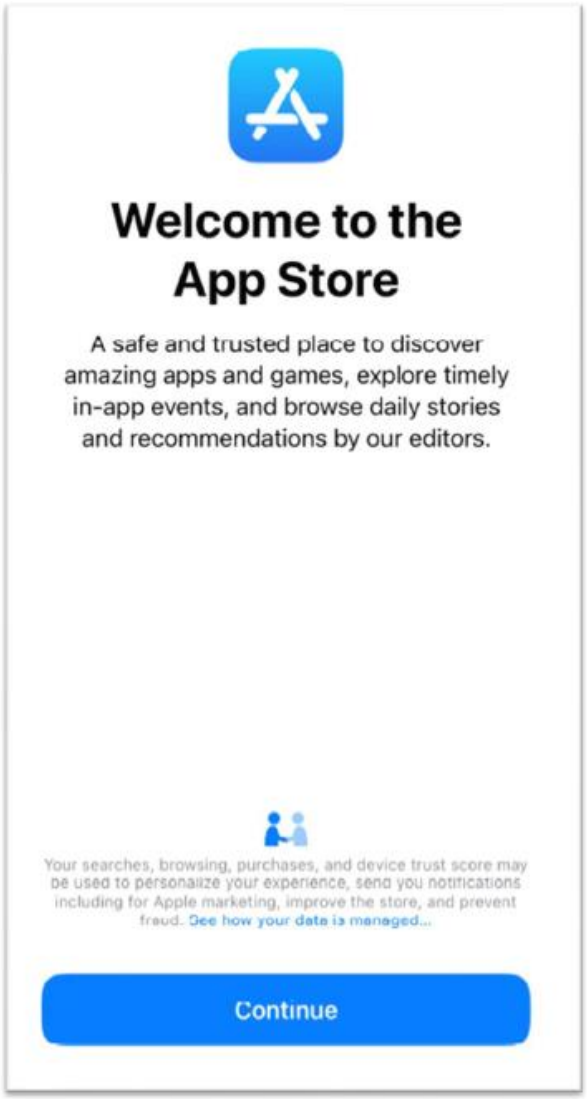
collection they now complain of. To use their devices, Plaintiffs were required to agree to the relevant software license. *See* RJN Ex. 1 at 1 ("BY USING YOUR DEVICE . . . YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE."); RJN Ex. 2 (watchOS Software License) at 1 (same). The software licenses incorporate Apple's Privacy Policy. CAC ¶ 103.

Apple's Privacy Policy, which "incorporates the mobile device's settings into the terms of the parties' agreement" (CAC ¶ 103), discloses the following:

> When you create an Apple ID, apply for commercial credit, purchase and/or activate a product or device, download a software update, register for a class at an Apple Store, connect to our services, contact us (including by social media), participate in an online survey, or otherwise interact with Apple, ***we may collect a variety of information***[.]

Id. ¶ 134 (quoting Apple's Privacy Policy) (emphasis in complaint).

The Privacy Policy also states that Apple may collect "usage data," which Apple defines as "[d]ata about your activity on and use of our offerings, such as app launches within our services, including browsing history; search history; product interaction; crash data, performance and other diagnostic data; and other usage data." RJN Ex. 3 ("Privacy Policy"). According to the Privacy Policy, Apple may also collect "device information," which Apple defines as "[d]ata from which your device could be identified, such as device serial number, or about your device, such as browser type. *Id.* For apps that provide media services—App Store, TV, Music, iTunes, Books, and Stocks—Apple collects additional data "to support the experiences users expect from these services." Mot. 10 (citing Privacy Policy). These apps provide additional disclosures when a user first opens that specific app. Below is an example of one of these "welcome screen" disclosures for the App Store. At the bottom of the screen, the disclosure states: "Your searches, browsing, purchases, and device trust score may be used to personalize your experience, send you notifications including for Apple marketing, improve the store, and prevent fraud." The disclosure then provides a link stating: "See how your data is managed," which when clicked, directs the user to additional disclosures about Apple's data collection.



RJN Ex. 4.

Consent "can be explicit or implied, but any consent must be actual." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 793 (N.D. Cal. 2022) (quoting *In re Google, Inc.*, No. 13-MD-02430, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013)). "In order for consent to be actual, the disclosures must 'explicitly notify' users of the practice at issue." *Id.* In determining consent, courts consider "whether the circumstances, considered as a whole, demonstrate that a reasonable person understood that an action would be carried out so that their acquiescence demonstrates knowing authorization." *Calhoun v. Google, LLC*, No. 22-16993, 2024 WL 3869446, at *5 (9th Cir. Aug. 20, 2024) (quoting *Smith*, 745 F. App'x at 8). If a user could have

plausibly understood the disclosures "as not disclosing that [the defendant] would engage in particular conduct," then the disclosures are insufficient to establish consent. *Id.*

The Court finds that Apple sufficiently disclosed the challenged data collection in both the Privacy Policy and then subsequently in the welcome screen disclosures. Plaintiffs allege that Apple collected (1) "what was tapped on, which Apps were searched for, what ads were displayed, how long an app was viewed, and how the app was found" (CAC ¶ 52); (2) "details about a user's mobile device . . . , including device identification numbers, what kind of device was used, the device's screen resolution, the device's keyboard language, and how the user was connected to the internet" (*id.*); and (3) "a 'Directory Services Identifier' that is tied to a mobile device user's iCloud account, and links their name, email address, and more to the harvested user data" (*id.* ¶ 55). The Privacy Policy discloses that Apple collects this very information. It explains that the App Store collects (or "logs") the following:

- Information "about your usage of the stores, including when you open or close the App Store, what content you search for, [and] the content you view and download" (RJN Ex. 9 at 2);
- Information related to "what you've previously searched for, viewed, downloaded, updated, or reviewed in the App Store" (*id.*);
- "[I]dentifiers such as your device's hardware ID and IP address" (*id.* at 1);
- "[T]ype of device, the version of your operating system, system, and the amount of free space on your device" (*id.* at 2);
- "[I]nformation about your browsing, purchases, searches, and downloads. These records may be stored with IP address, a random unique identifier (where that arises), and Apple ID when you are signed in to the App Store or other Apple online stores" (*id.* at 1).

Additionally, the welcome screens for each Apple App again disclose to users that "Your searches, browsing, purchases, and device trust score may be used to personalize your experience, send you notifications including for Apple marketing, improve the store, and prevent fraud." *See,*

e.g., RJN Ex. 4.

These combined disclosures are sufficient to establish that by using their devices, Plaintiffs, and "a reasonable person viewing those disclosures[,] would understand" and be on notice that Apple engaged in the contested data collection practices. *Smith*, 745 F. App'x at 8. "Courts consistently hold that terms of service and privacy policies, like [Apple's] privacy policy here, can establish consent to the alleged conduct challenged under various states wiretapping statutes and related claims." *Silver*, 2021 WL 3191752, at *4 (privacy policy which included provisions that disclose that parties may obtain various data provided sufficient notice of data collection).

Plaintiffs do not dispute they received sufficient notice of the collection. Rather, they contend that the software licenses disclosing the data collection are not part of the complaint. Opp. 6. The Court takes judicial notice of the software licenses for the reasons stated above. *See supra* Part III. Plaintiffs next respond that, even if the Privacy Policy and other notices disclose the collection at issue, any disclosure is modified by the statement in the same policy which permits users to withdraw their consent. Opp. 7 (citing CAC ¶ 48 ("Where you are requested to consent to the processing of your personal data by Apple, you have the right to withdraw your consent at any time")). And by disabling the "Allow Apps to Request to Track" and the "Share [Device] Analytics" settings, Plaintiffs assert that it was not unreasonable for them to assume this effectively withdrew consent to have Apple collect the contested data. *Id.* The Court will evaluate both settings in turn below.

a. "Allow Apps to Request to Track" Setting

As shown below, by enabling the "Allow Apps to Request to Track" setting, a user will "[a]llow apps to ask to track your activity across other companies' apps and websites."

RJN Ex. 16.

By disabling the "Allow Apps to Request to Track" setting, "all new app tracking requests are automatically denied." *Id.* This setting clearly applies to "activity across *other companies' apps and websites*"—by its plain language, the setting does not impact Apple's tracking activity across Apple Apps and websites. In other words, turning "off" the "Allow Apps to Request to Track" setting would not result in automatic denial of all new app tracking requests pertaining to activity across *Apple's* Apps; only activity across third party apps and websites. Additionally, by clicking on the "Learn more" link beneath the setting, users are presented with a disclosure titled "Tracking" (shown below) which states that "Apple requires app developers to ask for permission before they track your activity across apps or websites *they don't own* in order to target advertising to you, measure your actions due to advertising, or to share your information with data brokers." RJN Ex. 17 (emphasis added).

CAC ¶ 105.

Again, Apple notifies users that this setting relates to permission for app developers to track users' activity "across apps or websites [the app developers] don't own." This statement makes clear that the setting would not apply to Apple's tracking of users' activity across apps that Apple owns.

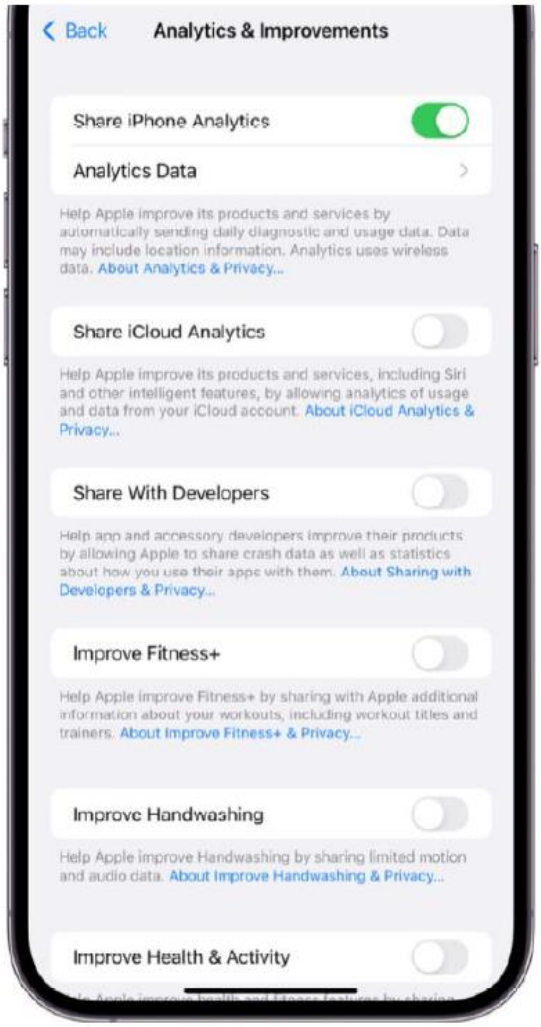
Despite this straightforward description of the setting's function, Plaintiffs contend that they believed disabling the setting would apply to Apple Apps. However, Plaintiffs do not explain why a reasonable person, reading the statements in the "Allow Apps to Request to Track" setting, would believe that turning the setting off would withdraw their consent to Apple's collection of data from Apple Apps. Plaintiffs merely argue that whether users could plausibly believe they were withdrawing their consent is highly factual and better reserved for a later stage. The Court finds that Plaintiffs' interpretation of the "Allow Apps to Request to Track" setting is implausible. That setting lets users choose whether apps can ask permission to track them across apps or websites owned *by other companies*—it does not affect data collection in Apple Apps that is not used to track users across other companies' sites.

Plaintiffs only challenge Apple's collection and tracking of their data while using Apple Apps. "[T]ak[ing] into account the level of sophistication attributable to the general public, which uses [Apple's] services," the "Allow Apps to Request to Track" setting unambiguously governs tracking of data not at issue here. *Calhoun v. Google, LLC*, 2024 WL 3869446, at *9.

Accordingly, even viewing the setting in the light most favorable to Plaintiffs, Plaintiffs' claim that they withdrew consent to the data collection at issue by turning off the "Allow Apps to Request to Track" setting is facially implausible, as that setting plainly does not govern the data collection Plaintiffs challenge here.

b. "Share [Device] Analytics" Setting

The "Share [Device] Analytics" setting, shown below, allows a user to control whether to share with Apple certain "Device Analytics" data.



RJN Ex. 15.

Beneath the option to "Share iPhone Analytics" is a statement that reads: "Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Data may include location information. Analytics uses wireless data." *Id.* at 1. The setting provides a

hyperlink where users can review another disclosure "[a]bout Analytics & Privacy." *Id.* The linked disclosure states, among other things, "[a]nalytics is designed to protect your information and enable you to choose what you share" and "iPhone Analytics may include details about hardware and operating system specification, performance statistics, and data about how you use your devices and applications." RJN Ex. 14 at 1. Plaintiffs allege that they "never consented to Apple tracking" their "confidential communications" while the "Share [Device] Analytics" setting was disabled. *See, e.g.*, CAC ¶ 11.

Apple argues that the "Share [Device] Analytics" setting concerns collection of technical performance data, such as data about app crashes or file compression effectiveness, and the disclosure's explanation of "Device Analytics" contradicts Plaintiffs' theory.[2] Mot. 13–14. Viewing the setting in the light most favorable to Plaintiffs, the Court cannot say that a reasonable user reading the "Share [Device] Analytics" setting must have understood that it did not control the data collection Plaintiffs complain of. The linked disclosure broadly states that iPhone Analytics "may include" "data about how you use your devices and applications." The disclosure also states that "[y]ou may choose to disable the sharing of Device Analytics altogether." It is plausible that a user reading this believed that by disabling the sharing of Device Analytics altogether, the user would no longer share, and Apple would no longer collect, "data about how [the user uses their] devices and applications." Unlike the "Allow Apps to Request to Track" setting, the "Share [Device] Analytics" setting is reasonably susceptible to more than one interpretation. At this stage, giving Plaintiffs the benefit of all reasonable inferences, Plaintiffs have plausibly alleged they believed they withdrew consent to the contested data collection by disabling the "Share [Device] Analytics" setting. *See In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 823 (N.D. Cal. 2020) (quoting *In re Facebook, Inc., Consumer Priv. User Profile*

[2] Apple also argues that Plaintiffs' purported understanding of these settings "defies common sense" because Apple Apps need certain data to provide the services and experiences users expect. Reply 6. At this stage, the Court declines to find that it would defy common sense for Plaintiffs to interpret the "Share [Devices] Analytics" setting as an opportunity to withdraw consent to the data collection at issue. Details regarding the type and scope of data collected can be addressed at a later stage.

Litig., 402 F. Supp. 3d 767, 789 (N.D. Cal. 2019) (where "the contract language at issue is reasonably susceptible to more than one interpretation, with one of those interpretations suggesting consent and another belying it, the Court cannot decide the consent issue in [Defendants'] favor").

* * *

The Court finds that Apple sufficiently disclosed the challenged data collection through the Privacy Policy and then subsequently in the welcome screen disclosures. However, Plaintiffs have plausibly alleged that they believed turning off the "Share [Device] Analytics" setting effectively withdrew their consent to challenged data collection—data about how Plaintiffs interact with Apple Apps. Plaintiffs have not plausibly alleged that the "Allow Apps to Request to Track" setting withdrew their consent. Accordingly, to the extent Plaintiffs' claims are based exclusively on the "Allow Apps to Request to Track" setting, the Court GRANTS Apple's motion to dismiss because Plaintiffs consented to the data collection. To the extent Plaintiffs' claims are based on the "Share [Device] Analytics" setting, the Court DENIES Apple's motion to dismiss because, although Apple disclosed the collection at issue, Plaintiffs plausibly alleged they withdrew their consent by turning off that setting.

B. Contract Claims

Apple moves to dismiss Plaintiffs' contract claims on several grounds. First, Apple contends Plaintiffs' breach of contract, implied contract, and implied covenant claims fail because Plaintiffs do not plead breach or damages. Second, Apple moves to dismiss the implied contract and unjust enrichment claims because Plaintiffs allege that an express contract governs. Third, Apple argues the implied covenant claim also fails because Plaintiffs do not allege that Apple unfairly prevented them from receiving a contracted-for benefit. Finally, Apple moves to dismiss the unjust enrichment claim because Plaintiffs do not allege any unjust act.

1. Breach

To plead a claim for breach of contract, Plaintiffs must allege: (1) the existence of a contract with Apple, (2) their performance under that contract, (3) Apple breached that contract,

and (4) they suffered damages. *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d at 831. Plaintiffs allege that Apple breached the Privacy Policy and Family Disclosure through promises made via Apple's settings. CAC ¶¶ 11–25, 103–14. Specifically, Apple allegedly breached the Privacy Policy and Family Disclosure based on Apple's "explicit promises" identified in Apple's settings that (1) refusing to "Allow Apps to Request to Track" would ensure that "all apps […] will be blocked from accessing the device's Advertising Identifier[;]" (2) disabling "Share [Device] Analytics" would prevent Apple from "sending daily diagnostic and usage data[;]"and (3) Apple would "not knowingly collect, use, or disclose any personal information from your child without your verifiable parental consent unless a COPPA exception applies." Opp. 10 (citing CAC ¶¶ 32–49, 103–13).

At the outset, Plaintiffs' breach of contract claim assumes that Apple's Privacy Policy "incorporates the mobile device's settings into the terms of the parties' agreements." CAC ¶ 102. Apple argues that the excerpted quote from the Privacy Policy which Plaintiffs rely on incorporates "the welcome screens and service-specific disclosures shown the first time a user opens an app," and *not* "the state of a user's settings." Mot. 14–15. But at this stage, the Court declines to interpret the Privacy Policy in favor of Apple.

Next, assuming the Privacy Policy incorporates the settings as pleaded, the Court turns to the individual alleged breaches. In connection with Apple's "Allow Apps to Request to Track" setting, Plaintiffs allege Apple breached its promise that it "requires app developers to ask for permission before they track your activity across Apps or websites they don't own" by "continuing to collect user data whenever Plaintiffs and the Class interacted with Apple's Apps." CAC ¶ 110. As explained above, Apple established the record supports finding that Plaintiffs consented to the complained of data collection, and Plaintiffs have not plausibly alleged they withdrew consent by turning off the "Allow Apps to Request to Track" setting because that setting unambiguously applies only to tracking of activity across Apps or websites which app developers "don't own"—tracking Plaintiffs do not challenge here. Accordingly, Plaintiffs have not plausibly stated a claim for breach of contract claim based on breach of the "Allow Apps to Request to

Track" setting. Although skeptical, the Court cannot determine that amendment would be futile and will give Plaintiffs an opportunity to amend.

Next, Plaintiffs argue that Apple breached its promise set forth in the "Share [Device] Analytics" setting, which states: "Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Data may include location information." CAC ¶ 107. By promising that disabling the setting would prevent Apple from "sending daily diagnostics and usage data," but collecting the usage data nevertheless, Apple purportedly breached its promise. Apple argues that disclosure relating to non-personal Device Analytics data cannot plausibly be interpreted to extend to *all* data collected by the apps to provide the content and services they offer. While Apple's interpretation of the "Share [Device] Analytics" setting may be the more realistic interpretation, the Court cannot determine that Plaintiffs' interpretation is implausible. At this stage, Plaintiffs have adequately alleged that Apple breached its promise in the "Share [Device] Analytics" setting, which Plaintiffs understood disabling would prevent Apple's collection of certain usage data.

Plaintiffs' final theory of breach is based on Apple's Family Disclosure, which applies only to minors under the age of 13. RJN Exs. 3, 18. The complaint fails to allege the ages of the two minor Plaintiffs. Thus, although Plaintiffs submit in opposing Apple's Motion that the minors are both under 13 years old, there is no factual basis in the complaint to conclude that Apple breached any promise that applied to the minor Plaintiffs. In opposing Apple's motion, Plaintiffs also assert that the minor Plaintiffs are third-party beneficiaries of the Family Disclosure. Opp. 13. Having failed to plead any third-party beneficiary theory in the complaint, Plaintiffs cannot avoid dismissal on this basis. *Jajco, Inc. v. Leader Drug Stores, Inc.*, 2013 WL 875957, at *1 (N.D. Cal. Mar. 7, 2013) (dismissing contract claim where the "complaint does not include allegations that [plaintiff] is an intended third party beneficiary").

In sum, Plaintiffs' breach of contract theory based on the "Allow Apps to Request to Track" setting and the Family Disclosure are both DISMISSED WITH LEAVE TO AMEND.

2. Damages

Having concluded that Plaintiffs' only cognizable theory of breach of contract is based on the "Share [Device] Analytics" setting, the Court proceeds to evaluate Apple's remaining arguments applied only to that theory. Apple argues that Plaintiffs have not plausibly plead "appreciable and actual damage" resulting from a breach. Mot. 15 (citing *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000)). Plaintiffs allege nominal damages, "the value of their data," and "the premium they paid for Apple mobile devices not to be tracked." CAC ¶¶ 57–84; Opp. 15. Recent authority instructs that under California law, "inability to show actual damages does not preclude recovery for breach of contract." *Raiser v. Ventura Coll. of L.*, 488 F. App'x 219, 222 (9th Cir. 2012); *see also Lundy v. Facebook Inc.*, 2021 WL 4503071, at *2 (N.D. Cal. Sept. 30, 2021) ("Nominal damages may be recovered for a breach of contract under California law"). Thus, Plaintiffs have sufficiently plead damages. The Court DENIES Apple's motion to dismiss Plaintiffs' contract claims on this basis.

3. Implied Contract, Unjust Enrichment, and Implied Covenant Claims

Apple moves to dismiss the implied contract and unjust enrichment claims because Plaintiffs contend an express contract governs the subject. "[T]here cannot be a valid, express contract and an implied contract, each embracing the same subject matter, existing at the same time." *Randall v. Univ. of the Pac.*, No. 5:20-CV-03196-EJD, 2022 WL 1720085, at *4 (N.D. Cal. May 28, 2022); *see also Nguyen v. Stephens Inst.*, 529 F. Supp. 3d 1047, 1057 (N.D. Cal. 2021) ("As a matter of law, a quasi-contract claim for unjust enrichment cannot lie where there exists between the parties a valid express contract covering the same subject matter") (quotations omitted).

Thus, an implied-in-fact contract may only arise if there is no express agreement between Plaintiffs and Apple. *Id.* Plaintiffs "may alternatively plead both a breach of contract claim and a quasi-contract claim, so long as [Plaintiffs] plead[] facts suggesting that the contract may be unenforceable or invalid." *Doe v. Regents of Univ. of Cal.*, 672 F. Supp. 3d 813, 821 (N.D. Cal. 2023). Plaintiffs have not done so. Rather, Plaintiffs argue that Apple's various marketing

statements "combined with the express terms of the contract documents" form the basis of an implied contract which Apple has breached. Opp. 14. In other words, Plaintiffs' implied contract claim relies in part on the same contractual documents underlying the breach of contract claim. Thus, Plaintiffs have failed to state a claim for breach of implied contract and unjust enrichment, and Apple's motion to dismiss Plaintiffs' breach of implied contract and unjust enrichment claim is GRANTED. Those claims are DISMISSED with leave to amend.

Apple further argues Plaintiffs' implied covenant claim fails because Plaintiffs identify no benefit of an express contract that Apple unfairly prevented them from receiving. Mot. 16. To state a claim for breach of the implied covenant of good faith and fair dealing, "a plaintiff must identify the specific contractual provision that was frustrated" by the defendant's conduct. *Perez v. Wells Fargo Bank, N.A.*, 2011 WL 3809808, at *18 (N.D. Cal. Aug. 29, 2011). Plaintiffs allege Apple "unfairly withheld the benefit of privacy" by collecting data when Apple's customers requested it refrain from such data collection. Opp. 14 (citing CAC ¶¶ 50–56).

Just as Plaintiffs have stated a claim for breach of contract with respect to the Apple's alleged failure to respect Plaintiffs' withdrawal of consent through the "Share [Device] Analytics" setting, Plaintiffs have stated a claim for breach of the implied covenant of good faith and fair dealing for that conduct. But as with Plaintiffs' breach of contract claim based on violation of the "Allow Apps to Request to Track" setting and the Family Disclosure, Plaintiffs have not stated a plausible claim for breach of the implied covenant based on that setting and the Family Disclosure.

Accordingly, Apple's motion to dismiss Plaintiffs' claim for breach of the implied covenant (along with the parallel claim for breach of contract) is GRANTED to the extent it is based on the "Allow Apps to Request to Track" setting and the Family Disclosure. Plaintiffs are permitted leave to amend.

C. Wiretap and Privacy Claims

1. CIPA

Count five of the complaint asserts a violation of the California Invasion of Privacy Act.

Cal. Penal Code §§ 630, *et seq.*; CAC ¶¶ 151–59. The CIPA is the California state law analogue to the federal Wiretap Act, enacted in 1967 in response to "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications." Cal. Penal Code § 630. Plaintiffs allege a violation of Section 632, which prohibits "intentionally and without the consent of all parties to a confidential communication, us[ing] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication." Cal. Penal Code § 632(a). Apple purportedly violated § 632 because it "designed, contrived and effectuated its scheme to track and record consumer communications while they were browsing Apps from their device while 'Allow Apps to Request to Track' and/or 'Share [Device] Analytics' were turned off." CAC ¶ 155.

Apple moves to dismiss the CIPA claim on several grounds.

Without consent. First, Apple argues Plaintiffs failed to satisfy the "without consent" element. As to the "Allow Apps to Request to Track" setting, the Court agrees Plaintiffs have not plausibly plead the data collection at issue was collected without consent for the reasons explained above. But the Court declines to dismiss the CIPA claim on this basis as to the "Share [Device] Analytics" setting. *See* supra Part IV(A)(2).

Device. Second, Apple argues the conclusory allegation that "Apple's mobile applications constitute an 'amplifying or recording device' under the CIPA" is not sufficient. CAC ¶ 157. Recent decisions in this Circuit have rejected Apple's interpretation and found that "software is a device under section 632(a)." *Doe v. Meta Platforms, Inc.*, 2023 WL 5837443, at *7 (N.D. Cal. Sept. 7, 2023); *see also Yockey v. Salesforce, Inc.*, No. 22-CV-09067-JST, 2024 WL 3875785, at *7 (N.D. Cal. Aug. 16, 2024) (agreeing that "software qualifies as a device under Section 632" and collecting cases). The Court finds those decisions persuasive. Plaintiffs have plausibly alleged that the Apple Apps at issue in this case constitute a "device" under Section 632.

Communication. Third, Apple contends Plaintiffs have not adequately alleged that the data collected is a "communication" within the meaning of CIPA. According to Apple, Plaintiffs do not specify what actions they took in any app or what data they believe was collected from

them, and so the complaint does not plausibly allege recording of a "communication." Mot. 18. As to what "communication" was recorded, Plaintiffs allege that, while browsing Apple's Apps, Apple recorded "what kind of device was used," the device's "screen resolution," the device's "keyboard language," in addition to what users "tapped on," which Apps were "searched" for, and how long an App was "viewed." CAC ¶¶ 52–55. While certain California courts have interpreted "communication" broadly to mean "the exchange of thoughts, messages or information by any means" (*People v. Gibbons*, 215 Cal. App. 3d 1204, 1208 (1989)), more recent California decisions "reflect[] an understanding that the term 'communication' for purposes of CIPA connotes a singular conversation or exchange shared between two or more participants." *Gruber v. Yelp Inc.*, 55 Cal. App. 5th 591, 607 (2020), as modified on denial of reh'g (Oct. 23, 2020). In the Court's view, it strains credulity to interpret "communication" for purposes of CIPA to include at least some of the data collection Plaintiffs complain of here, including information regarding the device's screen resolution, keyboard language, or how the user was connected to the internet. Plaintiffs cite two cases they contend support shoehorning this data into the definition of "communication" for purposes of CIPA. Opp. 18 (citing *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 795 and *Brown v. Google LLC*, 685 F. Supp. 3d 909, 934 (N.D. Cal. Aug. 7, 2023)). Neither persuade the Court. Initially, neither case directly addressed nor resolved the question of what constitutes a "communication" under CIPA. Rather, both evaluated whether the data collected in those cases were "content" within the meaning of the Wiretap Act. But even assuming those cases implicitly endorsed finding the data at issue constituted a "communication" under CIPA, the allegations in those cases were unlike those here. For instance, plaintiffs in *In re Meta* alleged that Meta intercepted electronic communications between plaintiffs and their healthcare providers, including full-string URLs that contained information which revealed the substance of patient communications with their health entities. *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 796 (transmitted URLs such as "hartfordhospital.org/services/digestivehealth/conditions-we-treat/colorectal-small-bowel-disorders/ulcerative-colitis" constituted "content" under Wiretap Act because they concern the

"substance of the communication"). And in *Brown*, plaintiffs alleged the intercepted communications contained the users' IP addresses, referers, user-agents, HTTP requests, users' actions on a website, and their search queries. *Brown*, 685 F. Supp. 3d at 935 (referring to example of full-string URL from which Google would know "that the user was searching for updates on Russia's war against Ukraine").

Here, Plaintiffs' allegations lack similar detail from which the Court can conclude the alleged collection constitutes a "communication" under CIPA. Without more, Plaintiffs have failed to plausibly allege the requisite recording of a communication, and Apple's motion to dismiss count five is GRANTED. Plaintiffs are permitted leave to amend. The Court need not evaluate Apple's remaining arguments as to this count.

2. WESCA

Count seven of the complaint asserts a violation of Pennsylvania's Wiretapping and Electronic Surveillance Control Act. WESCA prohibits the intentional interception of the contents of any electronic communication (18 Pa. C.S. § 5703) and "operates in conjunction with and as a supplement to the Federal Wiretap Act." *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125– 26 (3d Cir. 2022). Apple argues Plaintiffs' WESCA claim should be dismissed for failing to allege any of the required elements. Mot. 20. First, WESCA permits interception "where all parties to the communication have given prior consent to such interception." Having found Apple disclosed the collection at issue, and Plaintiffs plausibly allege withdrawal of that consent based on the "Share [Device] Analytics" setting (but not the "Allow Apps to Request to Track" setting), the Court declines to dismiss the WESCA claim based on prior consent.

Second, Apple argues Plaintiffs have not alleged an "interception" under WESCA because Apple did not obtain the "contents" of any "communication." WESCA's definition of "contents" —"any information concerning the substance, purport, or meaning of that communication" (18 Pa. C.S. § 5702)—is similar to the Wiretap Act's definition of "contents" and the term is "interpretated in the same way" in both statutes. *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 n.6 (3d Cir. 2003). Not included in the scope of "content" is "record" data like "basic

identification and address information" because this information does not constitute "the substance, purport, or meaning" of communications. *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (user's Facebook ID and the address of the webpage from which the user's HTTP request to view another webpage was sent not considered "content" under Wiretap Act). As explained above in the context of whether the collected information constituted a "communication" under CIPA, Plaintiffs' allegations similarly lack sufficient detail to infer that the information collected amounted to more than just "record" data. Plaintiffs allege Apple intercepted "what was tapped on, which Apps were searched for, what ads were displayed, how long an app was viewed, and how the app was found," along with "details about a user's mobile device." CAC ¶ 52.

In *James v. Walt Disney*, the plaintiffs alleged that Oracle intercepted "information about the webpages they viewed and searches they conducted." 701 F. Supp. 3d 942, 956 (N.D. Cal. Nov. 8, 2023). While recognizing that intercepting "mouse clicks and keystrokes" would likely not rise to the level of "contents" under WESCA because that information does not reveal the substance of any communication, the court did conclude that information about the webpages plaintiffs' viewed and searches they conducted was sufficient. *Id.* Here, consistent with the cases interpreting WESCA's "content" requirement, the only information that might plausibly reveal the substance of any communication under WESCA is information regarding "which Apps were searched for." CAC ¶ 52. Although "[u]nder some circumstances, a user's request to a search engine for specific information" could constitute content, without more detail regarding whether Plaintiffs searched for specific information, this is not one of those circumstances.[3] *In re Zynga Priv. Litig.* at 1108. The remaining collected information (*e.g.*, what was tapped on, what ads were displayed, how long an app was viewed, the device screen resolution) lacks requisite detail to convince the Court that it might plausibly reveal the substance of any communication rather than

[3] The Court is not suggesting that Plaintiffs are required to plead the exact Apps that were searched for. However, Plaintiffs must plead, as in *Brown* and *In re Meta*, at least *some* detail to allow the Court to evaluate the information contained in the purported intercepted communications and whether the information is more than "record" data.

convey "record" data WECSA does not protect.

Plaintiffs fail to adequately allege the collection of "content"—a required element to plead a violation of WESCA. Accordingly, the Court GRANTS Apple's motion to dismiss Plaintiffs' WESCA claim. Plaintiffs are permitted leave to amend.

D. Invasion of Privacy

Count four of Plaintiffs' complaint asserts an invasion of privacy under California's Constitution. CAC ¶¶ 138–50. To state a claim for invasion of privacy under the California Constitution, Plaintiffs must show that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is "so serious ... as to constitute an egregious breach of the social norms" such that the breach is "highly offensive." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). Apple argues Plaintiffs fail to plead all three elements. In evaluating the sufficiency of an invasion of privacy claim, courts ask whether (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive. *Id.*

Apple contends Plaintiffs fail to plead a reasonable expectation of privacy because (1) Plaintiffs consented to the collection, and (2) Plaintiffs cannot reasonably expect that data they knowingly provide to Apple would not be received by Apple. Mot. 23. The Court rejects Apple's first argument because Plaintiffs plausibly alleged they withdrew their consent to the data collection based on the "Share [Device] Analytics" setting (but not the "Allow Apps to Request to Track" setting). For its second argument, Apple cites *United States v. Forrester*, where the Ninth Circuit held that internet users "have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit" because "they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." 512 F.3d 500, 510 (9th Cir. 2008). In a similar vein, Apple argues that reasonable consumers understand when they buy a book in the Books app, for example, Apple must record the purchase to process the transaction and make the book available on users' devices. Mot. 23. The Court agrees. No reasonable consumer would expect to engage

in a transaction with Apple without *some* data being collected from Apple to process that transaction. While the Court declines to rule at this stage on *which* data consumers would reasonably expect to be collected, as plead, the complaint has not plausibly alleged a reasonable expectation of privacy. To be sure, courts in the Ninth Circuit have recognized a reasonable expectation of privacy related to certain data collection. *See In re Facebook*, 956 F.3d at 603 (allegations that Facebook "collects a full-string detailed URL, which contains the name of a website, folder and sub-folders on the web-server, and the name of the precise file requested" sufficient to plead a reasonable expectation of privacy); *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1232 (C.D. Cal. 2017) (plaintiffs have cognizable interest in keeping "detailed data about what video content they watch private"); *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1077 (N.D. Cal. 2021) (allegations that Google collected "a complete, cradle-to-grave profile of users" sufficient to plead a reasonable expectation of privacy). The allegations of Apple's data collection here fall short of those in the above cases—particularly because Plaintiffs allege Apple collected data from Plaintiffs' interactions with *Apple's own apps*. Plaintiffs have failed to sufficiently plead that they had any reasonable expectation of privacy in Apple's data collection, and Apple's motion to dismiss the invasion of privacy claim is GRANTED with leave to amend.[4]

E. Consumer Protection Claims

Plaintiffs allege violations of California, New York, New Jersey, and Illinois consumer protection laws. CAC ¶¶ 160–74 (UCL); *id.* ¶¶ 194–216 (GBL); *id.* ¶¶ 240–256 (NJCFA); *id.* ¶¶ 257–281 (ICFDA). The parties agree each claim requires a fraudulent statement or deceptive act. Mot. 26; Opp. 26. Because each claim sounds in fraud, Plaintiffs must meet Rule 9(b)'s heightened pleading standard. Plaintiffs allege Apple misrepresented its commitment to privacy and the safety of users' data via Apple's (1) "Allow Apps to Request to Track" and "Share

[4] The Court need not address whether the disclosed data collection is an "egregious breach" of social norms, but the Court is skeptical Plaintiffs have alleged sufficient factual detail regarding the data collection at issue to rise to the requisite level.

[Device] Analytics" settings, and (2) statements made in various Apple marketing materials.

1. Settings

Starting with the two settings, Plaintiffs have not plausibly alleged they withdrew consent by turning off the "Allow Apps to Request to Track" setting because that setting unambiguously applies only to tracking of activity across Apps or websites which app developers "don't own." Thus, any misrepresentation claims based on that setting fail because Plaintiffs only allege improper collection of their data on *Apple's* Apps. As to the "Share [Device] Analytics" setting, Apple again argues that this setting governs certain device performance data which is not at issue here. But for the reasons stated above, Plaintiffs have plausibly alleged that disabling the setting would "disable the sharing of Device Analytics," which may "include [...] data about how you use your devices and applications." CAC ¶¶ 46–47. This is sufficient to plead a misrepresentation.

In addition to alleging a misrepresentation, Plaintiffs must allege reliance on the statement in order to plead a cause of action for fraud in California. *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1126 (9th Cir. 2009). Plaintiffs have sufficiently done so. *See* CAC ¶ 169. Apple argues that Plaintiffs have not alleged "which specific statement, advertisement, or representation they viewed or when." Reply 18. But this overlooks Plaintiffs' allegations about the specific "Share [Device] Analytics" setting, and how Plaintiffs understood that disabling the setting would de-activate the data tracking feature on their phones. CAC ¶ 169. Moreover, at the motion to dismiss stage, "actual reliance ... is inferred from the misrepresentation of a material fact." *Moore v. Mars Petcare US, Inc.*, 966 F.3d 1007, 1021 (9th Cir. 2020) (quoting *Friedman v. AARP, Inc.*, 855 F.3d 1047, 1055 (9th Cir. 2017)). And whether a misrepresentation is sufficiently material to allow for an inference of reliance is "generally a question of fact that cannot be decided at the motion to dismiss stage." *Id.* Here, for the reasons stated above, it is plausible that a reasonable consumer would (1) believe that disabling the "Share [Device] Analytics" setting meant Apple would not collect the data at issue, and (2) rely on the "Share [Device] Analytics" setting.

2. Marketing Campaign

With respect to the advertisements and other marketing statements, Plaintiffs allege that

"Apple aggressively markets that it protects privacy" and refers to billboards with statements such as "Privacy. That's iPhone," "We're in the business of staying out of yours," "Privacy is King," and "Our apps mind their business. Not yours." Under appropriate factual circumstances, a representative consumer plaintiff "may not be able to pinpoint the exact portion of a long-standing, widespread advertising campaign he or she relied on when purchasing a product." *Yastrab v. Apple Inc.*, 173 F. Supp. 3d 972, 980 (N.D. Cal. 2016). That said, it is nevertheless not enough to "nebulously reference a product's advertising package and just declare the campaign misleading." *Id.* Here, Plaintiffs point broadly to Apple's "purported privacy commitments" and contend that Apple "claims to offer its mobile device users the option to control what data app developers can collect by adjusting their device's privacy settings." CAC ¶ 44. But Plaintiffs do not allege what is false or misleading about Apple's marketing materials and why those materials were misleading vis-à-vis Plaintiffs' complained of data collection. *See In re iPhone 4s Consumer Litig.*, No. C 12-1127 CW, 2014 WL 589388, at *5 (N.D. Cal. Feb. 14, 2014), *aff'd sub nom. In re iPhone 4s Consumer Litig.*, 637 F. App'x 414 (9th Cir. 2016) ("Rule 9(b) therefore requires Plaintiffs to aver specifically the statements they relied upon in making their purchases, what is false or misleading about the statements, and why those statements turned out to be false"). Although Plaintiffs sufficiently allege what Apple promises when the privacy setting is engaged (CAC ¶¶ 44–49) and how they believe that promise was supposedly false (*id.* ¶¶ 50–52), they do not similarly allege what is false or misleading about the advertisements and why those advertisements turned out to be false. Moreover, only some of the Plaintiffs allege that they saw or read any of the advertisements or marketing statements. For example, Bruce Puleo alleges he "was exposed to advertisements from Apple touting the company's commitment to privacy" (CAC ¶ 13), but others make no similar claim. *See, e.g., id.* ¶ 11; *see In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *37 (N.D. Cal. May 27, 2016) (dismissing affirmative misrepresentation claim where none of the eleven plaintiffs alleged "they saw, read, or—for that matter—even knew about [defendant's] privacy policies prior to the data breach").

Accordingly, Plaintiffs' consumer law claims based on the advertisements are not plead

with particularity. Apple's motion to dismiss the consumer protection claims based on a misrepresentation is GRANTED with respect to the advertisements and the "Allow Apps to Request to Track" setting but DENIED with respect to the "Share [Device] Analytics" setting. Plaintiffs are permitted leave to amend.

3. Omission Theory

In addition to Apple's misrepresentations in the two settings and advertising campaign, Plaintiffs allege Apple's omissions concerning Plaintiffs' privacy violated the consumer protection statutes. *See, e.g.*, CAC ¶ 167. To the extent Plaintiffs' omission theory relies on the "Allow Apps to Request to Track" setting, it fails to state a plausible claim. As explained above, Apple discloses the disputed data collection, and that setting unambiguously does not apply to Apple Apps. Because Plaintiffs do not plausibly allege they withdrew their consent from the disclosed data collection, Apple's Privacy Policy and welcome screens do disclose the complained-of data collection.

Apple also argues Plaintiffs failed to allege with particularity that, had Apple made specific disclosures, Plaintiffs would have been aware of them and would not have purchased their devices. Mot. 28 (citing *Tabak v. Apple, Inc.*, No. 19-CV-02455-JST, 2020 WL 9066153, at *9 (N.D. Cal. Jan. 30, 2020)). The Court agrees. Plaintiffs "need not prove that the omission was the only cause or even the predominant cause, only that it was a substantial factor in [their] decision." *Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1225 (9th Cir. 2015). But Plaintiffs here make only conclusory allegations they "would not have purchased their devices from [Apple] or would have paid less for them." *See, e.g.*, CAC ¶ 171. As in *Tabak*, where plaintiffs alleged that they "would not have purchased the devices at issue if they had known about the defect," the allegations here lack specific factual matter to raise the reasonable inference that, had Apple disclosed information about the data collection at issue, Plaintiffs "would have been aware of it and behaved differently." *Tabak*, 2020 WL 9066153, at *9 (quoting *Daniel*, 806 F.3d at 1225). In response, Plaintiffs argue that Apple "was obliged to disclose this collection" because Apple was in a "superior position to know" about how it used the data. Opp. 27 (quoting *Donohue v. Apple, Inc.*,

871 F. Supp. 2d 913, 926 (N.D. Cal. 2012)). But even so, Plaintiffs must still include some detail beyond conclusory statements that would suggest that disclosure of the data collection would have played a role in Plaintiffs' decision to purchase the devices at issue. Thus, Plaintiffs have not sufficiently alleged a plausible fraudulent omission claim. Apple's motion to dismiss the consumer protection claims based on a fraudulent omission theory is GRANTED. Plaintiffs are permitted leave to amend.

4. California UCL

Apple separately moves to dismiss Plaintiffs' UCL claim because Plaintiffs "have not alleged a misrepresentation or omission with particularity required by Rule 9(b)" and thus cannot satisfy UCL's "fraudulent" or "unlawful" prongs. Mot. 29. The Court found that Plaintiffs have sufficiently plead at least a misrepresentation based on the "Share [Device] Analytics" setting. Thus, Apple's motion to dismiss on this basis fails. As for the "unfair" prong, Apple argues Plaintiffs have not identified a specific constitutional, statutory, or regulatory provision to which their claim is tethered. Mot. 30 (citing *Drum v. San Fernando Valley Bar Ass'n*, 182 Cal. App. 4th 247, 257 (2010)). And regarding the "unlawful" prong, Apple argues Plaintiffs' passing references to COPPA in the complaint fails to sufficiently plead how Apple violated that, or any other, law. Plaintiffs do not challenge these apparent defects, and the Court will GRANT Apple's motion to dismiss Plaintiffs' UCL claim based on the "unfair" and "unlawful" prongs with leave to amend. *Adam Askari D.D.S. Corp. v. U.S. Bancorp*, No. 5:21-CV-09750-EJD, 2022 WL 2161603, at *3 (N.D. Cal. June 15, 2022) ("By failing to respond to those arguments, Plaintiff has conceded them and acknowledged the Complaint should be dismissed on those grounds as well").

5. Damages

Apple also moves to dismiss the consumer protection claims because Plaintiffs do not allege cognizable damages. Mot. 28–29. Each of Plaintiffs' asserted consumer protection claims require the loss of money or property. *See Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 739–40 (7th Cir. 2014) (ICFDA requires "actual damages"); *Small v. Lorillard Tobacco Co.*, 94 N.Y.2d 43, 56 (1999) (GBL requires "either pecuniary or 'actual' harm"); *Kwikset Corp. v. Super.*

Ct., 51 Cal. 4th 310, 323 (2011) (UCL requires "lost money or property"); *Solo v. Bed Bath & Beyond, Inc.*, 2007 WL 1237825, at *3 (D.N.J. Apr. 26, 2007) (NJCFA requires "ascertainable loss of moneys or property").

Plaintiffs allege Apple "deprived Plaintiffs and Class Members of the economic value of their user data" (CAC ¶ 84) and Plaintiffs "would not have purchased Apple's devices and/or used Apple's Apps" (*id.* ¶ 208) or paid a "premium price to other equivalent phones" for Apple's devices (*id.* ¶ 209). Regarding the economic value of Plaintiffs' data lost, courts in this district appear split regarding whether privacy harms involving personal data can constitute an injury to money or property sufficient to provide standing under the UCL. *Compare In re Facebook Priv. Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011), *aff'd* 572 F. App'x 494 (9th Cir. 2014) ("[P]ersonal information does not constitute property for purposes of a UCL claim") and *M.K. v. Google LLC*, No. 21-cv-08465-VKD, 2023 WL 2671381, at *5 (N.D. Cal. Mar. 27, 2023) (same) *with In re Meta Pixel Tax Filing Cases*, No. 22-CV-07557-PCP, 2024 WL 1251350, at *24 (N.D. Cal. Mar. 25, 2024) (privacy harms can constitute economic injury to confer UCL standing under three theories: unfair benefit-of-the-bargain to businesses who violate user expectations about how their data will be used, diminished value of personal information, and reduced right to exclude others from accessing personal data) and *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) ("plaintiffs who suffered a loss of their personal information suffered economic injury and had standing").

Even assuming privacy harms involving personal data *can* constitute an injury to money or property sufficient to provide standing under the UCL, the Court is not convinced Plaintiffs have adequately alleged such harm here. "[J]ust because Plaintiffs' data is valuable in the abstract, and because [Apple] might have made money from it, does not mean that Plaintiffs have 'lost money or property' as a result." *Hazel v. Prudential Fin., Inc.*, No. 22-CV-07465-CRB, 2023 WL 3933073, at *6 (N.D. Cal. June 9, 2023) (dismissing UCL claim for failing to allege lost money or property); *see also In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d at 804 (dismissing UCL claim and explaining that "Facebook may have gained money through its

sharing or use of the plaintiffs' information, but that's different from saying the plaintiffs lost money"). Indeed, courts find allegations regarding loss of value of personal data sufficient where the loss is somehow tethered to plaintiffs. *See Brown v. Google LLC*, No. 20-CV-03664-LHK, 2021 WL 6064009, at *15 (N.D. Cal. Dec. 22, 2021) (alleged loss of PII value sufficient under UCL where "each named Plaintiff has alleged that he or she is aware of" platforms willing to pay individuals for data); *see also In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *14 (N.D. Cal. Aug. 30, 2017) (same where plaintiffs alleged their "PII is being sold by hackers on the dark web, and that Plaintiffs have lost the value of their PII as a result").

Here, Plaintiffs allege that their personal user information is valuable in the abstract and that they have suffered "loss of value in their personally identifiable information." CAC ¶¶ 68–69, 158. Plaintiffs recognize that their internet browsing history "can be quantified, because technology companies have been willing to pay users for the same or substantially the same user data at issue here." *Id.* ¶ 69 (citing studies showing certain contact information valued at $4.20 a year). Although internet browsing history, or other personally identifiable information, can be quantified or sold, Plaintiffs do not allege they intended to sell the data Apple collected or otherwise allege that someone else would have bought the data. *See Lau v. Gen Digital Inc.*, No. 22-CV-08981-JST, 2023 WL 10553772, at *7 (N.D. Cal. Sept. 13, 2023) (UCL claims dismissed where plaintiffs do not allege that "they ever attempted or intended to participate" in the market for the information allegedly collected and stored by defendants, "or otherwise to derive economic value from" that information). Although the Court finds insufficient Plaintiffs' allegations that Apple "deprives Plaintiffs and Class Members of the economic value of their user data" under UCL, Apple has not shown such allegations are insufficient under the other consumer protection laws. *See* Mot. 29. The Court therefore declines to find the allegations insufficient under the GBL, ICFDA, or NJCFA based on Plaintiffs' loss of the value of their PII.

Plaintiffs also allege they would not have purchased Apple's devices or used the Apps, or would have paid less for Apple's devices had they known about the data collection at issue. *See,*

e.g., CAC ¶¶ 208, 209. These conclusory allegations, untethered in any way to Plaintiffs' experiences, are insufficient to plead damages under the consumer protection laws. *See Naimi v. Starbucks Corp.*, 798 F. App'x 67, 70 (9th Cir. 2019) ("[u]nder New York law, a plaintiff's allegation that she would not have purchased a product but for a deceptive act, standing alone, is not a cognizable injury because it conflates the deceptive act with the injury."); *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 740 (7th Cir. 2014) (plaintiff failed to plead actual damage for ICFDA claim where plaintiff alleged "without any factual support, that he paid more than the value of the [product]"); *Gerritsen v. FCA US LLC*, No. CV 19-08268-AB (KSX), 2020 WL 3841304, at *1 (C.D. Cal. Mar. 3, 2020) (conclusory allegations of overpayment insufficient to state injury under UCL); *White v. Samsung Elecs. Am., Inc.*, No. CV 17-1775, 2019 WL 8886485, at *3 (D.N.J. Aug. 21, 2019) (allegations that plaintiff "would not have purchased, or would have paid substantially less for" product had she known of misrepresentation insufficient to plead NJCFA claim).

* * *

Apple's motion to dismiss Plaintiffs' UCL claim is GRANTED for failing to allege cognizable damages. Plaintiffs' UCL claim based on (1) misrepresentations made via Apple's advertisements and the "Allow Apps to Request to Track" setting, (2) fraudulent omissions made by Apple, and (3) a violation of the "unfair" or "unlawful" prongs also fails for reasons stated above, and Apple's motion to dismiss Plaintiff's remaining consumer protection claims is DENIED because Apple has not established the allegations insufficient under the GBL, ICFDA, or NJCFA based on Plaintiffs' loss of the value of their PII.

F. Equitable Relief

Finally, Apple argues the Court lacks equitable jurisdiction to hear Plaintiffs' UCL and unjust enrichment claims because Plaintiffs fail to plead inadequate legal remedies. Mot. 30 (citing *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020)) for proposition that Plaintiffs "must establish that [they] lack[] an adequate remedy at law before securing equitable restitution for past harm under the UCL and CLRA"). Plaintiffs respond that, at this stage, they

sufficiently plead that they lack an adequate remedy at law. Opp. 29 (citing CAC ¶ 287). The Court agrees. Courts in this district typically permit the pursuit of alternative remedies at the pleadings stage. *Steiner v. Vi-Jon Inc.*, No. 23-CV-00473-AMO, 2024 WL 1181002, at *7 (N.D. Cal. Mar. 18, 2024) (collecting cases). The complaint alleges that legal remedies "are inadequate because they are not equally certain and prompt as equitable relief," and "[d]amages are not equally certain as restitution insofar as the Court may award restitution even if it determines that insufficient evidence is provided to support an award of damages." CAC ¶ 287. The Court finds this sufficient at the pleading stage, and Apple's motion is DENIED on this basis. But as explained above (*see supra* Part IV(A)(2)), Plaintiffs' unjust enrichment theory based on the "Allow Apps to Request to Track" setting is DISMISSED because Apple disclosed the collection at issue, and Plaintiffs' interpretation of that setting is implausible. *See Hicks v. PGA Tour, Inc.*, 897 F.3d 1109, 1120 n.6 (9th Cir. 2018) (affirming dismissal of unjust enrichment claim based on consent).

V. CONCLUSION

For the foregoing reasons, the Court rules as follows:

- To the extent Plaintiffs' claims, other than Plaintiffs' claim for violation of ICFDA, are based exclusively on the "Allow Apps to Request to Track" setting, the Court GRANTS Apple's motion to dismiss.
- All claims are DISMISSED WITH LEAVE TO AMEND, except for the following claims, which are permitted to proceed for the reasons outlined above:
    - Plaintiffs' count one for breach of express contract based on the "Share [Device] Analytics" setting;
    - Plaintiffs' count three for breach of implied covenant of good faith and fair dealing based on the "Share [Device] Analytics" setting;
    - Plaintiffs' counts eight and nine for violation of New York's GBL based on purported misrepresentations made via Apple's "Share [Device] Analytics" setting;

- Plaintiffs' count ten for violation of NJCFA based on purported misrepresentations made via Apple's "Share [Device] Analytics" setting;
- Plaintiffs' count eleven for violation of ICFDA based on misrepresentations made via Apple's "Share [Device] Analytics" and "Allow Apps to Request to Track" setting; and
- Plaintiffs' count twelve for unjust enrichment based on the "Share [Device] Analytics" setting.

Any amended complaint must be filed within 30 days.

IT IS SO ORDERED.

Dated: September 26, 2024

EDWARD J. DAVILA
United States District Judge

United States District Court
Northern District of California