UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE APPLE DATA PRIVACY LITIGATION

Case No. 5:22-cv-07069-EJD

ORDER GRANTING MOTION TO DISMISS

Re: ECF No. 150

Plaintiffs[1] bring this putative class action against Defendant Apple, Inc. ("Apple") for allegedly improper collection and use of Apple mobile device users' data. Plaintiffs allege that Apple collects this data when users interact with Apple's proprietary, first-party applications ("apps")—*e.g.*, the App Store, Apple Music, Apple TV, Books, and Stocks—on their mobile Apple devices. First Am. Compl. ¶¶ 1–6, ECF No. 148 ("FAC"). Further, Plaintiffs claim that Apple misled users into believing that certain settings would restrict Apple's collection, storage, and use of private data, when in reality, the settings did no such thing.

Currently before the Court is Apple's motion to dismiss the FAC under Rules 9(b) and 12(b)(6). The motion is fully briefed, and the Court heard oral argument on October 9, 2025. Opp., ECF No. 152; Reply, ECF No. 153; ECF No. 158. After careful consideration of the parties' briefing and arguments, the Court **GRANTS** Apple's motion.

I. BACKGROUND

The Court previously summarized the facts of this case in its Order dismissing Plaintiffs'

[1] Bruce Puleo, Carlina Green, David Sgro, A.H. (a minor), Dottie Nikolich, Elena Nacarino, Francis Barrott, Katie Alvarez, E.M. (a minor), and Quincy Venter.

first consolidated complaint. MTD Order at 1–3, ECF No. 138. The core facts have not changed and do not bear repeating.

There are, however, a few notable differences between Plaintiffs' original consolidated complaint and the FAC that are relevant to the instant motion. First, the number of named plaintiffs has decreased from fifteen in the original complaint to ten in the FAC. *Compare* ECF No. 115 at 2, *with* FAC at 2. Second, Plaintiffs proceed only with claims based on the "Share [Device] Analytics" setting and abandon their reliance on the "Allow Apps to Request to Track" setting. Finally, Plaintiffs reassert claims the Court dismissed in the MTD Order and assert a new claim under Cal. Penal Code § 638.51, the pen register provision of the California Invasion of Privacy Act ("CIPA").

II. LEGAL STANDARD

To survive Apple's motion, the FAC "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible when the facts alleged allow the Court to draw the reasonable inference that the defendant is liable for the alleged misconduct beyond a mere possibility. *Id.* The Court does not, however, accept conclusory allegations or draw unreasonable inferences from the allegations. *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (citation omitted). Claims that sound in fraud must satisfy the heightened pleading standard of Rule 9(b), meaning that they must be specific enough to give the defendant notice of the particular misconduct and allege the "who, what, when, where, and how" of the alleged misconduct. Fed. R. Civ. P. 9(b); *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124–25 (9th Cir. 2009).

III. REQUEST FOR JUDICIAL NOTICE

Before turning to the merits of Apple's motion, the Court addresses Apple's supplemental request for judicial notice in support of its motion. RJN, ECF No. 151. When deciding a Rule 12(b)(6) motion, the Court may consider documents outside of the complaint that are incorporated by reference or subject to judicial notice. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988,

998 (9th Cir. 2018). Under the incorporation by reference doctrine, courts may incorporate documents or portions thereof that are not expressly referenced in the complaint if they form the basis of the plaintiff's claims, or the claims depend on documents' contents. *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005). Courts may also take judicial notice of certain facts that are "not subject to reasonable dispute" because they are "generally known" or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b).

Here, Apple requests that the Court treat as incorporated by reference or take judicial notice of four documents in addition to the seventeen documents the Court considered when deciding Apple's previous motion to dismiss. *See* MTD Order at 6–9. The four documents Apple asks the Court to consider now are copies of (1) the welcome screen that appears when opening the Game Center service; (2) the Game Center settings screen; (3) the Game Center & Privacy disclosure dated January 27, 2025; and (4) the Game Center Developer webpage. RJN, Exs. 19-22, ECF Nos. 151-2–151-5. Plaintiffs did not file an opposition to Apple's RJN.

The Court finds that Exhibits 19 through 22 are properly subject to incorporation by reference or judicial notice for the same reasons the Court articulated in the MTD Order. Exhibits 19 and 20 are not cited in the FAC but are still incorporated by reference because they form the basis of Plaintiffs' claims and "relate to whether Apple disclosed its collection practices and whether Plaintiffs consented to these collection practices." MTD Order at 8. Exhibits 21 and 22 are Apple's publicly-available online privacy policies and terms, of which courts regularly take judicial notice. *See, e.g., id.*; *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1068 n.3 (N.D. Cal. 2016). Accordingly, the Court will consider Exhibits 19 through 22 in addition to the Exhibits the Court recognized in the prior MTD Order.

IV. DISCUSSION

Apple seeks dismissal of several claims asserted in the FAC: violation of CIPA § 632 (eavesdropping or recording confidential communication), violation of CIPA § 638.51 (use of a pen register), violation of Pennsylvania's Wiretapping and Electronic Surveillance Act

("WESCA"), invasion of privacy under the California Constitution, and violation of California's Unfair Competition Law ("UCL"), breach of implied contract, and unjust enrichment. Apple also requests that the Court dismiss allegations in the FAC regarding Apple's Game Center. The Court addresses each issue in turn, beginning with Plaintiffs' new claim under CIPA's pen register provision.

A. CIPA § 638.51

Section 638.51 of CIPA prohibits the "install[ation] or use [of] a pen register or a trap and trace device without first obtaining a court order pursuant to Section 638.52 or 638.53." Cal. Penal Code § 638.51. The statute defines the term "pen register" to mean "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." *Id.* § 638.50(b). Apple contends that Plaintiffs do not and cannot invoke the pen register statute for several reasons.

1. Identification of a Pen Register

First, Apple argues that Plaintiffs fail to identify a pen register. Section 638.51 defines "pen register" as capturing information "transmitted by an *instrument* or *facility*." Cal. Penal Code § 638.50(b) (emphases added). As such, Apple contends that the pen register must be something separate from the instrument or facility that transmits the communications. Applied here, this interpretation renders implausible Plaintiffs' allegation that Apple's apps are pen registers, because the apps are themselves the source of the communications. Plaintiffs do not necessarily dispute Apple's reading of the statute but argue that Apple misconstrues the FAC, because it is the "processes within Apple's Apps, not the applications as a whole, that operate as pen registers." Opp. at 15.

Plaintiffs' theory runs into several problems. First and foremost, the theory Plaintiffs lay out in their opposition brief is not what they allege in the FAC. Plaintiffs specifically allege that "*Apple's mobile applications* constitute a 'pen register' because they are devices or processes that record addressing or signaling information . . . from the electronic communications transmitted by

their devices." FAC ¶ 186 (emphasis added). Plaintiffs' allegations clearly identify Apple's apps as the recording devices or processes, not some undefined processes within those apps, and Plaintiffs may not amend the FAC through their brief. *Apple Inc. v. Allan & Assocs. Ltd.*, 445 F. Supp. 3d 42, 59 (N.D. Cal. 2020). Perplexingly, Plaintiffs seemed to change their theory once again at the hearing on Apple's motion to dismiss. When asked whether Plaintiffs believe Apple's apps or some process within the apps are the alleged pen register, Plaintiffs stated that "it's both . . . [because] the application is inherently a collection of processes." 10/9/2025 Hearing Tr. at 28:6-11, ECF No. 160. This more closely aligns with the FAC's allegations but still leaves Plaintiffs' theory of liability unclear at best.

Even if Plaintiffs had pled their process theory in the FAC, it would still fail to state a claim. The Court agrees with Apple that the statute's definition of "pen register" necessarily applies only to a device or process separate from the source of the transmitted communications. To interpret the statute otherwise would lead to absurd results. For example, if read the other way, the pen register statute would create criminal liability for call logs on cell phones because the logs list routing information like the phone numbers called from a particular phone. Plaintiffs' argument that the alleged pen register is the processes running Apple's apps as opposed to the apps themselves is a distinction without difference, because it does not change the fact that both are a part of the same "instrument or facility" that is the source of the communication.

Still, Plaintiffs argue that other courts have interpreted the term "pen register" broadly to include "processes that record users' IP addressing information, but not the content of the electronic communications being transmitted from users' computers or smartphones," a definition that easily encompasses the app processes here. Opp. at 15–16 (citing *Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 928 (N.D. Cal. 2024); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023)). Plaintiffs contend that *Greenley* and *Shah* stand for the rule that "courts should focus less on the form of the data collector and more on the result." *Shah*, 754 F. Supp. 3d at 928 (quoting *Greenley*, 685 F. Supp. 3d at 1050). The Court agrees with this proposition as a general matter, but *Greenley* and *Shah* are inapposite. In those cases, the alleged pen registers were third-

party trackers that were embedded in websites and intercepted communications between the user and the website, so it was clear that the pen register was separate from the source of the communication. *Greenley*, 685 F. Supp. 3d at 1032; *Shah*, 754 F. Supp. 3d at 928. Not so here. Apple's first-party apps and their underlying processes are a part of the source of the transmitted communications, which is enough to disqualify them from being pen registers. Accordingly, failure to identify a pen register under the statute's definition is one ground for dismissing Plaintiffs' Section 638.51 claim.

2. Application to Internet Communications

Apple next argues that Section 638.51 only regulates collection of telephone information and should not be extended to internet data. Apple notes that the statute explicitly references use of a pen register for collecting information from telephones, so it cannot apply to other technologies as a matter of statutory interpretation.

The California Supreme Court instructs that when interpreting statutory provisions, "each sentence must be read not in isolation but in the light of the statutory scheme," so "[a]n interpretation that renders related provisions nugatory must be avoided." *Lakin v. Watkins Associated Indus.*, 6 Cal. 4th 644, 659 (1993). Here, Apple contends that applying the pen register statute to internet communications runs afoul of this principle. Apple observes that another provision in the statute requires any court order authorizing use of a pen register to "specify . . . [t]he number and, if known, physical location of the *telephone line* to which the pen register . . . is to be attached." Cal Penal Code § 638.52(d)(3) (emphasis added). Extending Section 638.51 to internet communications would render this provision "nugatory." Indeed, recent decisions from California state courts have agreed. *See, e.g.*, *Sanchez v. Cars.com Inc.*, 2025 WL 487194, at *3 (Cal. Super. Jan. 27, 2025) (rejecting extension of CIPA's pen register provision to internet communications based on the statutes' "plain language and legislative intent"); *Casillas v. Transitions Optical, Inc.*, 2024 WL 4873370, at *2 (Cal. Super. Sept. 9, 2024) ("Section 638.50 does not address the privacy rights of Internet users.").

However, many federal district courts, including those in this District, have interpreted the

pen register statute in the manner proposed by Plaintiffs. These courts rejected the argument that CIPA's pen register definition applies only to telephone technology, citing "the expansive language in the California's Legislature's chosen definition [of pen register]," which is "specific as to the type of data the pen register collects . . . but [] vague and inclusive as to the form of the collection tool." *Greenley*, 684 F. Supp. 3d at 1050; *see also Shah*, 754 F. Supp. 3d at 928 (citing *Greenley*); *Mirmalek v. Los Angeles Times Commc'ns LLC*, No. 24-CV-01797, 2024 WL 5102709, at *3 (N.D. Cal. Dec. 12, 2024) (same).

Considering this apparent split in authority regarding the proper interpretation of Section 638.51, the question of whether the pen register statute applies outside of the telephone context is a close call. Both readings apply sound statutory interpretation principles but reach different results. Without the benefit of further developments in caselaw on this issue, the Court is at this time inclined to follow what is currently the majority rule in federal district courts. Accordingly, the pen register statute applies to internet communications and does not bar Plaintiffs' claim here.

3. Application to Private Entities

Apple's next related argument is that the pen register provision only applies to law enforcement and not private entities. Section 638.51 prohibits the installation or use of a pen register, unless "a person . . . obtain[s] a court order obtained pursuant to Section 638.52 or 638.53." Cal. Penal Code § 638.51(a). Section 638.52 and 638.53, in turn, provide guidelines for "peace officers" or law enforcement officers seeking such an order. *Id.* §§ 638.52, 638.53. Apple argues that CIPA's pen register provision therefore only applies to law enforcement officers.

The Court disagrees. Though the requirements for court orders in Sections 638.52 and 638.52 apply only to law enforcement officers, Section 638.51 is not so narrow. The plain language of Section 638.51 suggests that it applies to the broader category of "persons" as opposed to only "peace officers." *People v. Adir Int'l, LLC*, 114 Cal. App. 5th 275 (2025) ("When the Legislature uses different words as part of the same statutory scheme, those words are presumed to have different meanings." (quoting *Romano v. Mercury Ins. Co.*, 128 Cal. App. 4th 1333, 1343 (2005)). Read together, the statute prohibits any person's installation or use of a pen

register but carves out a narrow exception for peace officers who receive authorization to do so via court order. *Shah*, 754 F. Supp. 3d at 930 (holding that § 638.52 "does not alter the definition of a pen register. Instead, that section lists the procedures that law enforcement officers must follow when applying for a pen register.") This interpretation still comports with the legislative purpose of Section 638.51: "to create a comprehensive framework governing how California law enforcement officials could obtain and use a pen register or trap and trace device, just like its federal counterpart." *Sanchez*, 2025 WL 487194, at *3.

4. Contradictory Causes of Action

Lastly, Apple argues that Plaintiffs' Section 638.51 claim fails because it contradicts their Section 632 claim. The definition of "pen register" for Section 638.51 covers devices or processes that record "dialing, routing, addressing, or signaling information" and explicitly excludes those that record "the contents of a communication." Cal. Penal Code § 638.50(b). Meanwhile, Section 632 prohibits eavesdropping on or recording the substance of "confidential communication[s]," which excludes "non-content-based conduct coincident to the communication." *People v. Drennan*, 84 Cal. App. 4th 1349, 1356 (2000). Collection of the same communications thus cannot simultaneously violate both provisions.

Yet, Apple contends that Plaintiffs allege just that in the FAC. Plaintiffs' Section 632 claim asserts that Apple's apps recorded their "communications," and Plaintiffs' Section 638.51 claim asserts that the same apps recorded only the "dialing, routing, addressing, or signaling information." *Compare* FAC ¶¶ 162–63, *with id.* ¶ 186. Plaintiffs' first response to this is that there is no contradiction because certain processes within the app act as the pen register while others record the content of the communications. But as explained above, Plaintiffs did not plead this new process theory in the FAC, and they may not amend their complaint through briefing. Stuck with their allegation that it is Apple's apps, not the processes therein, that record user data, Plaintiffs admit that the apps "collect a variety of information – some of which are 'communications' and some which are 'routing, addressing, or signaling information.'" Opp. at 19.

Plaintiffs attempt to still salvage these contradictory claims by arguing that Plaintiffs are permitted to plead their pen register claim in the alternative under Federal Rule of Civil Procedure 8(d)(3). While that may be true, Plaintiffs have not done so in the FAC. Plaintiffs did not indicate that they plead their pen register claim as an alternative to their Section 632 claim. In fact, in their pen register claim, Plaintiffs expressly "incorporate[d] by reference and re-allege[d] each and every allegation set forth in paragraphs 1 through 105" (FAC ¶ 182), including their allegation that Apple's apps captured "confidential communications" (*id.* ¶¶ 11–20). These inconsistent allegations and causes of action are another ground for dismissal of Plaintiffs' pen register claim. *U.S. Med. Instruments, Inc. v. CFS N. Am., Inc.*, 2013 WL 6055387, at *9 (S.D. Cal. Nov. 13, 2013) ("The Ninth Circuit has held that where inconsistent allegations are not pled in the alternative, but are expressly incorporated into each cause of action, an allegation may constitute a judicial admission by the plaintiff which allows dismissal of the complaint.") (citing *Maloney v. Scottsdale Ins. Co.*, 256 F. App'x 29, 31 (9th Cir. 2007)).

* * *

In sum, Plaintiffs fail state a claim for violation of CIPA's pen register provision. The Court therefore GRANTS Apple's motion to dismiss this claim. Given the deficiencies identified in this Order, the Court doubts that Plaintiffs can plead a viable claim under the pen register statute. But since this is the first time Plaintiffs have asserted this claim, the Court grants leave to amend.

B. CIPA § 632

In the FAC, Plaintiffs reassert their claim for violation of CIPA section 632. Section 632 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 contends that Plaintiffs' claim fails once again, because Plaintiffs do not plead that the data Apple allegedly collected was "confidential" or a "communication" or that Apple engaged in eavesdropping or recording.

1. Confidential

Section 632 defines "confidential communication" to exclude circumstances in which the parties "may reasonably expect that the communication may be . . . recorded." Cal. Penal Code § 632(c). As such, California courts presume that internet communications do not give rise to a reasonable expectation of privacy, in part because they are written communications that are by their very nature recorded. *Revitch v. New Moosejaw, LLC*, No. 18-CV-06827, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (collecting cases); *Boulton v. Community.com, Inc.*, No. 23-3145, 2025 WL 314813, at *2 (9th Cir. Jan. 28, 2025) (holding that text messages that are "by nature recorded" cannot be "confidential" communications under Section 632).

Apple contends that this presumption applies here. As internet-connected applications, Apple's apps operate using the client-server model, in which client devices—here, Plaintiffs' mobile devices—request services from Apple's servers that then record the request and transmit the requested information back to the client devices. These device-to-server transmissions are "by their very nature recorded on the [device] of at least the recipient" and thus are not "confidential" communications under Section 632. *See In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *23 (N.D. Cal. Sept. 26, 2013) (emails not "confidential" under Section 632).

Plaintiffs do not dispute that Apple's apps operate in this manner. They instead assert that their withdrawal of consent by turning off the "Share [Device] Analytics" setting created a reasonable expectation that none of their usage data[2] would be sent to Apple.

The Court disagrees. Consumers may hold a subjective expectation that no usage data would be sent to Apple, but that expectation is objectively unreasonable. As the Court stated in in its previous Order, "[n]o reasonable consumer would expect to engage in a transaction with Apple without *some* data being collected from Apple to process that transaction." MTD Order at 29–30. The same continues to apply with equal force here. Plaintiffs allege Apple collects myriad data points that fall under the definition of "usage data," but almost all of this data is of the kind one

[2] Plaintiffs rely on Apple's definition of "usage data," which includes browsing history, search history, product interaction, crash data, performance and other diagnostic data, and other usage data. FAC ¶ 41.

would expect Apple would need to collect in order to respond to Plaintiffs' requests. *See* FAC ¶¶ 55–59.

Plaintiffs specifically focus on Apple's collection of referral URLs and search terms, but neither change the result. For Apple to respond appropriately to a user's request, it must record the requested referral URL or search terms on its servers, and Plaintiffs fail to explain how such data collection is unnecessary. The cases Plaintiffs rely upon are distinguishable from the instant one, because they dealt with third-party tools used for intercepting an alleged communication between a user and the intended recipient. *See In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 799 (N.D. Cal. 2022); *Smith v. YETI Coolers, LLC*, 754 F. Supp. 3d 933, 939, 943 (N.D. Cal. 2024); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 596 (9th Cir. 2020). Plaintiffs' reliance on turning off the "Share [Device] Analytics" setting does not justify a departure from the presumption that first-party internet communications are not confidential. As such, Plaintiffs have not sufficiently alleged that any communication Apple collected was "confidential."

2. Communication

Though CIPA itself does not define "communication," the California Court of Appeal has interpreted the term to mean "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). The exact contours of this definition are still somewhat undefined, but it is clear that "communication" refers to the substance or content of an exchange of ideas, not the "non-content-based conduct coincident to the communication." *People v. Drennan*, 84 Cal. App. 4th 1349, 1358 (2000). This interpretation is consistent with the legislative purpose behind the statute: to prevent "intrusion on one's thoughts, ideas, or knowledge." *Id.; Cf. In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (holding that "contents" of an online communication for purposes of the federal Wiretap Act "refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication")

The Court previously dismissed Plaintiffs' Section 632 claim because their allegations

lacked detail from which the Court could conclude that the information Apple collected was "communication." MTD Order at 26. The Court held that much of the information Apple allegedly collected—the kind of mobile device used, the device's screen resolution, the device's keyboard language, what users tapped on, which apps users searched for, and how long an app was viewed—fell into the bucket of "non-content-based conduct coincident to the communication" as opposed to part of the "communication" itself. *Id.* at 26–27; *see Drennan*, 84 Cal. App. 4th at 1358.

Plaintiffs contend that the FAC now contains enough specificity to satisfy the "communication" element of their Section 632 claim. Specifically, Plaintiffs argue that "URLs of referral websites that open [Apple's] Apps, including URLs from healthcare providers and financial institutions . . . [as well as] users' gender, user agent, IP latitude, IP longitude, IP city, referral app name, destination URL, search terms, and user actions" fit the bill. Opp. at 13–14 (citing FAC ¶¶ 12, 54–60).[3]

As an initial matter, user agent, IP latitude, IP longitude, IP city, and user actions are the same kinds of data the Court already found not to be "communication" in the MTD Order, because they pertain to *how*, not *what* information is relayed. MTD Order at 26–27 (explaining that "what users 'tapped on'" and "how the user was connected to the internet" fell outside the scope of "communication"). Plaintiffs' continued reliance on *Brown v. Google LLC* is misplaced. 685 F. Supp. 3d 909 (N.D. Cal. 2023). There, too, the court held that "users' IP addresses and their user-agents, [are] the record, not substance, of the communication." *Id.* at 935.

Search terms and URLs, on the other hand, may constitute "communication" if the data convey the user's inner thoughts and ideas. *Cf. In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 795 (N.D. Cal. 2022) (finding that URLs such as "hartfordhospital.org/services/digestivehealth/conditions-we-treat/colorectal-small-bowel-

[3] Plaintiffs also contend that the "communications" in their allegations pertain only to transmitted data that is unnecessary for any Apple app to function. Opp. at 8. The Court addresses this issue in the context of whether Plaintiffs alleged the collected data was "confidential." *See supra* Section III.B.1.

disorders/ulcerative-colitis" are "content" under Wiretap Act because they disclose the "substance of the communication"); *Brown*, 685 F. Supp. 3d at 935 (same for URL that revealed "that the user was searching for updates on Russia's war against Ukraine"). However, Plaintiffs have not shown that that is the case here. Plaintiffs mostly allege that they searched for apps and stock symbols by name, but simply searching for app titles on the App Store or stock symbols does not necessarily convey thoughts and ideas. That information is more akin to browsing apps and stocks than exchanging a user's substantive information. *Cf. Vita v. New England Baptist Hosp.*, 243 N.E.3d 1185, 1199 (Mass. 2024) ("Browsing and accessing the information published on a website is significantly different from having a conversation or sending a message to another person."). And though Plaintiffs allege that Apple collected the URLs of referral and destination websites, Plaintiffs have not pled the specific text of those URL, so the Court is unable to infer that they contained users' thoughts and ideas. These deficiencies doom most of Plaintiffs' allegations of "communication."

There is, however, one exception. Plaintiff Carlina Green alleges that she used search terms such as "roommate," "LSAT," "screen time," and "used cars." FAC ¶ 12. These search terms go beyond browsing specific apps on the App Store to reveal her inner thoughts and interests. Accordingly, the Court finds that only Plaintiff Green has alleged that Apple collected her "communication" under Section 632.

3. Eavesdropping or Recording

Section 632 also requires "eavesdrop[ping] upon or record[ing]" confidential communication. Cal. Penal Code § 632(a). Plaintiffs do not contend that Apple "eavesdrops" but maintain that Apple records their confidential communications. Apple does not dispute that its servers record user data but argues that Section 632 applies only to a person who "uses" a recording device and not to a company like Apple receiving data transmissions that are by nature recorded on servers. Reply at 8 (citing *Boulton*, 2025 WL 314813 at *2). The sole authority Apple cites for this proposition, however, does not state that a company like Apple cannot "record" communications under Section 632. *Boulton* only stands for the rule that data

transmissions that are by nature recorded cannot be "confidential communications." Accordingly, Plaintiffs have sufficiently pled that Apple recorded their communication for purposes of Section 632.

* * *

In sum, Plaintiffs have not adequately pled a claim under CIPA Section 632. Their allegations do not overcome the presumption that the data Apple collects is "confidential." Nor have Plaintiffs sufficiently pled that the collected data constitute a "communication," with the exception of the search terms that Plaintiff Green used in the App Store. The Court therefore GRANTS dismissal of Plaintiffs' Section 632 claim.

C. WESCA

WESCA prohibits the intentional interception of the contents of any electronic communication using a device (18 Pa. C.S. §§ 5702–03) 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 that Plaintiffs again fail to state a WESCA claim because (1) Plaintiffs have not pled that Apple collected the "contents" of any communication; (2) Plaintiffs fail to allege collection by a "device"; and (3) Apple was the direct recipient of any communication.

1. Contents

Under WESCA, "contents" means "any information concerning the substance, purport, or meaning of that communication." 18 Pa. C.S. § 5702. This definition is identical to the Federal Wiretap Act's definition of "contents," and identical terms in the two statutes are "interpreted in the same way." *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 n.6 (3d Cir. 2003). As noted above (*supra* Section III.B.2), the "contents" of an online communication under the Wiretap Act are "the intended message conveyed by the communication, [which] does not include record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga*, 750 F.3d at 1106.

The Court previously dismissed Plaintiffs' WESCA claim because their allegations

"lack[ed] sufficient detail to infer that the information collected amounted to more than just 'record' data." MTD Order at 28. In the FAC, the sole Pennsylvania plaintiff, David Sgro, alleges that he searched for Zoom, Brave Browser, Instagram, and pdf scanner in the App Store and accessed other apps in the App Store through third-party websites. *Id.* ¶ 13. For the same reasons discussed above (*see supra* Section III.B.2), search terms do not constitute "contents" when the terms are simply the titles of particular apps on the App Store. And without any allegations about the specific text of referral URLs from third-party websites, the Court cannot discern how such data would convey the "substance, purport, or meaning" of any communication." 18 Pa. C.S. § 5702. Thus, Plaintiffs do not adequately allege the collection of "contents."

2. Device

A "device" under WESCA means "[a]ny device or apparatus . . . that can be used to intercept a wire, electronic or oral communication." 18 Pa. C.S. § 5702. Plaintiffs allege that their mobile devices are the intercepting devices (FAC ¶ 202),[4] but Apple argues that cannot be, since the device performing the interception must be separate from the source of the communication. The Court agrees. Though WESCA does not explicitly state so, it would make little sense for the device that transmits the communication to also be the intercepting device. *See Commonwealth v. Diego*, 119 A.3d 370, 374 (Pa. Super. Ct. 2015) (rejecting argument that the device that was "the origin of the intercepted message" could be the same as "the device that purportedly intercepted that message"). Plaintiffs thus fail to allege an intercepting "device" under WESCA.

3. Direct-Party Exception

Apple also argues that Plaintiffs' WESCA claim cannot proceed because Apple was the direct recipient of communication, and where "a party receives information from a communication

[4] Puzzlingly, Plaintiffs once again contradict their allegations in the FAC by arguing that "Apple's Apps (and the processes therein) are the intercepting devices." Opp. at 20–21. The FAC clearly alleges that "Apple's mobile devices (e.g., iPhones, iPads, and Apple Watches)" are the relevant devices. FAC ¶ 202. The Court will disregard Plaintiffs' argument that Apple's apps or any processes are "devices" for purposes of WESCA as another improper attempt to amend the FAC through briefing. *See Apple Inc. v. Allan & Assocs. Ltd.*, 445 F. Supp. 3d 42, 59 (N.D. Cal. 2020).

as a result of being a direct party to the communication, there is no interception." *Commonwealth v. Proetto*, 771 A.2d 823, 831 (Pa. Super. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003); *see also Commonwealth v. Cruttenden*, 58 A.3d 95, 98–100 (Pa. 2012). Apple urges the Court not to follow the Third Circuit's decision in *Popa v. Harriet Carter Gifts, Inc.*, a case Plaintiffs cite in their opposition, because that holding was a non-binding "prediction." 52 F.4th 121 (3d Cir. 2022).

In *Popa*, the Third Circuit interpreted a 2012 amendment to WESCA as abrogating the direct-party exception outside of narrow circumstances involving law enforcement. *See id.* at 128 (holding that "the Pennsylvania legislature decided to codify a specific, narrow intended-recipient exemption for law enforcement, limiting *Proetto* and *Cruttenden* to their facts"). The circuit court reasoned that a broader direct-party exception would run contrary to another part of the statute that allows interception only where all parties to the communication consent. *Id.* This holding was not mere prediction; the Third Circuit was persuaded that Pennsylvania Supreme Court would agree with the circuit court's interpretation. *Id.* at 129. Likewise, this Court sees no reason to divert from the Third Circuit's sound interpretation of the amended WESCA. The Court therefore rejects the argument that the direct-party exception applies here to immunize Apple from WESCA liability.

For the foregoing reasons, the Court GRANTS Apple's motion to dismiss Plaintiffs' WESCA claim.

D. California Constitution Invasion of Privacy

To state a claim for invasion of privacy under the California Constitution, Plaintiffs must plausibly allege that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) Apple's intrusion is "so serious . . . as to constitute an egregious breach of the social norms" such that it is "highly offensive." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020). Though Apple contends that Plaintiffs have not pled any of the three elements, courts often focus on the second and third elements when testing the sufficiency of a California invasion of privacy claim. *Id.*

Here, the Court need only reach the second element of whether Plaintiffs have a reasonable expectation of privacy. When dismissing Plaintiffs' invasion of privacy claim last time, the Court found that "[n]o reasonable consumer would expect to engage in a transaction with Apple without *some* data being collected from Apple to process that transaction," but stopped short of deciding exactly *which* data consumers should reasonably expect to be collected by Apple. MTD Order at 29–30. Plaintiffs contend they have now amended their allegations to address this issue. Plaintiffs argue reasonable consumers would not expect Apple to collect data that is "unnecessary" for the functionality of Apple's apps—the user's gender, birth year, IP latitude, IP longitude, and URL—especially given that Plaintiffs withdrew consent to Apple's collection of usage data by turning off the "Share [Device] Analytics" setting. Opp. at 22–23.

Plaintiffs' allegations still miss the mark. In determining whether a plaintiff has a reasonable expectation of privacy, courts consider the sensitivity of the data and the context in which the data was allegedly collected. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 603 (holding that whether plaintiffs have a reasonable expectation of privacy in collected data depends on "whether the data itself is sensitive *and* whether the manner it was collected . . . violates social norms"); *see also Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1077 (N.D. Cal. 2021) (considering "the amount of data collected, the sensitivity of the data collected, and the nature of the data collection"). The Court already found it plausible that turning off the "Share [Data] Analytics" setting would create a reasonable expectation that Apple would not collect some user data. But Plaintiffs' current argument that this reasonable expectation of privacy covers data that is "unnecessary" to the functioning of Apple's apps is unconvincing for a couple of reasons. First, Plaintiffs do not clearly differentiate in their allegations what data are "necessary," and which are "unnecessary," nor do they substantiate the premise that Apple's apps do not require the "unnecessary" data elements to function. IP latitude and IP longitude, for example, are required by certain apps that provide location-specific services. And date of birth is likewise necessary for apps providing age-restricted services.

Second, even if they had made a clear distinction, Plaintiffs have not demonstrated that the

data they deem "unnecessary" is highly sensitive. Plaintiffs raise URLs as an example of highly sensitive data that Apple collects and claim that the Court has already found URLs to be data in which consumers would have a reasonable expectation of privacy. Plaintiff's reliance on the MTD Order is misplaced. As the Court stated previously, URLs can be constitutionally problematic if they reveal information about a user's internet activity. *See United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008). But more general URLs that do not reveal more personal information, such as www.apple.com, do not raise the same issues. Plaintiffs have not pled enough in the FAC for the Court to plausibly infer that data Apple allegedly collected contained the type of detailed personal information that courts have found to be highly sensitive.

Indeed, the data collection Plaintiffs complain of here is different in kind and degree to the data collection courts have found to support a reasonable expectation of privacy. In *Facebook Internet Tracking*, a case that Plaintiffs liken to their own, Facebook allegedly acquired "highly personalized profiles from sensitive browsing histories and habits." 956 F.3d at 604. In *Brown*, another case Plaintiffs rely upon, Google allegedly collected internet activity while in private browsing mode that "may reveal: a user's dating history, a user's sexual interests and/or orientation, a user's political or religious views, a user's travel plans, a user's private plans for the future." 525 F. Supp. 3d at 1077–78. Plaintiffs do not allege that Apple collected any such data. Moreover, as the Court pointed out in the MTD Order, Plaintiffs' allegations concern data Apple allegedly collected from Plaintiffs' interactions with *Apple's own apps*. MTD Order at 30. It is difficult to see how consumers would have a reasonable expectation of privacy in this context.

Accordingly, the Court GRANTS dismissal of Plaintiffs' constitutional invasion of privacy claim.

E. California UCL

Apple next challenges the sufficiency of Plaintiffs' renewed UCL claim. Apple argues that Plaintiffs' FAC fails to remedy the three deficiencies which led the Court to dismiss the UCL claim in the first consolidated complaint: failure to allege (1) economic injury, (2) an omission with the particularity required by Rule 9(b), and (3) a violation of the "unfair" or "unlawful"

prongs. Because Plaintiffs have made minimal amendments to address the first requirement in the FAC, the issue is dispositive of Plaintiffs' UCL claim, and the Court need not reach Apple's other arguments.

To have statutory standing to bring their UCL claim, Plaintiffs must allege they lost money or property as a result of Apple's alleged unfair competition. Cal. Bus. & Prof. Code § 17204; *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 323 (2011). In the FAC, Plaintiffs make the same allegations regarding damages as they did in the first consolidated complaint: (1) Apple "deprived Plaintiffs and Class Members of the economic value of their user data without providing proper consideration" (FAC ¶ 90); and (2) Plaintiffs "seek damages for the price premium paid to [Apple] for their Apple mobile devices" (*id.* ¶ 181), and "would not have purchased their devices from Defendant or would have paid less for them" (*id.* ¶ 178). The Court previously found these allegations insufficient to establish standing to bring UCL claims. MTD Order at 34–37. As to the user data theory, Plaintiffs only plead that their data is valuable in the abstract and fail to allege that they had any intention to sell the data Apple allegedly collected. *See id.* at 36. And as to the price premium theory, Plaintiffs still rely on conclusory allegations untethered to their own experiences. *See id.* at 37. The Court therefore GRANTS Apple's motion as to Plaintiffs' UCL claim for the same reasons the Court dismissed the claim in the first consolidated complaint.

F. Implied Contract and Unjust Enrichment

The Court dismissed Plaintiffs' original implied contract and unjust enrichment claims because these claims relied on the express contracts underlying Plaintiffs' breach of contract claim. MTD Order at 23–24. As the Court explained, "there 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.*, 2022 WL 1720085, at *4 (N.D. Cal. May 28, 2022). The Court acknowledged that 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), but found that Plaintiffs had not done so in their complaint. Apple argues that Plaintiffs

have not remedied these deficiencies in the FAC.

Plaintiffs counter that they have adequately pled a breach of implied contract in the alternative this time around. Yet, as Apple notes, the FAC is devoid of any allegation that Plaintiffs' express contract with Apple is unenforceable or invalid. Without facts even suggesting as much, Plaintiffs still have not adequately pled their implied contract and unjust enrichment claims. The Court thus GRANTS Apple's motion to dismiss these claims.

G. Game Center Allegations

Finally, Apple asks the Court to dismiss any allegations concerning Apple's Game Center. Apple argues that Game Center is not an app (RJN, Ex. 22, ECF No. 151-5), and none of the Plaintiffs allege that they themselves used Game Center (FAC ¶¶ 11–20), so any claims based on Game Center must be dismissed. Plaintiffs counter that Game Center was previously an app and that they included Game Center in the FAC "to highlight that Apple collects the same type of data across all of its Apps." Opp. at 27. Regardless of whether Game Center is an app, Plaintiffs do not dispute that they have not pled that Apple used Game Center to collect *their* data. This defect dooms any of their claims based on Game Center. *See Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1188 (N.D. Cal. 2020). Accordingly, Court GRANTS Apple's motion to dismiss all of Plaintiffs' claims based on Game Center.

V. CONCLUSION

For the foregoing reasons, the Court **GRANTS** Apple's motion. Plaintiffs' CIPA Section 638.51, CIPA Section 632, WESCA, constitutional invasion of privacy, UCL, implied contract, and unjust enrichment claims are dismissed. The Court also dismisses any claims based on Apple's Game Center without prejudice to Plaintiffs' amending their complaint to plead that Game Center collected their data.

It is doubtful whether Plaintiffs can sufficiently plead their dismissed claims given the deficiencies addressed in this Order, which have remained despite Plaintiffs' having had an opportunity to amend. However, the Court **GRANTS** leave to amend once more out of an abundance of caution. Any amended complaint must be filed within 30 days of this Order.

IT IS SO ORDERED.

Dated: January 20, 2026

EDWARD J. DAVILA
United States District Judge