BURSOR & FISHER, P.A.
L. Timothy Fisher (SBN 191626)
Brittany S. Scott (SBN 327132)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com
bscott@bursor.com

LYNCH CARPENTER, LLP
(Eddie) Jae K. Kim (SBN 236805)
ekim@lcllp.com
Tiffine E. Malamphy (SBN 312239)
tiffine@lcllp.com
117 East Colorado Blvd., Suite 600
Pasadena, CA 91105
Telephone: (626) 550-1250
Facsimile: (619) 756-6991

Interim Co-Lead Counsel

[Additional counsel appear on signature page]

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

IN RE: APPLE DATA PRIVACY LITIGATION

Case No. 5:22-cv-07069-EJD
(Consolidated)

PLAINTIFFS' OPPOSITION TO APPLE'S MOTION TO DISMISS

Date: March 21, 2024
Time: 9:00 a.m.
Courtroom 4 -5th Floor
Judge: Hon. Edward J. Davila

TABLE OF CONTENTS

PAGE(S)

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

RULES

OTHER AUTHORITIES

Plaintiffs 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"), by and through their undersigned counsel, hereby respectfully submit this brief in opposition to Defendant Apple, Inc.'s ("Defendant" or "Apple") Motion to Dismiss ("MTD") (ECF No. 122).

INTRODUCTORY STATEMENT OF FACTS

Plaintiffs bring this class action against Apple for the 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—on their mobile Apple devices (i.e., iPhone, iPad, or Apple Watch). Consolidated Class Action Complaint ("CAC") (ECF No. 115) ¶¶ 1-6. Plaintiffs allege that Apple promised their customers privacy, but misled users that certain settings would restrict Apple's collection, storing, and use of private data, when in fact Apple disregarded these choices and collected, stored, and used the data anyway. CAC ¶¶ 1-6.

For years, 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. CAC ¶¶ 32-34. Apple emblazoned billboards of the iPhone with the slogan "Privacy. That's iPhone" and ran the ads across the world for months. CAC ¶¶ 33-43. The Apps are advertised as implicitly not collecting user data. *See, e.g.,* CAC ¶ 35 ("We're staying in the business of staying out of yours."); ¶ 36 ("Our apps mind their business. Not yours."); ¶ 40 ("Your iPhone knows a lot about you. But we don't".). Consistent with its advertisements, Apple promised mobile device users that they would have control over Apple's collection of their personal data. CAC ¶¶ 44-49. For example, 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. In its "App Tracking Transparency" disclosure, Apple states that it allows device users "to choose whether an app can track your activity across other companies' Apps and websites for the purposes of advertising or sharing with data brokers." CAC ¶¶ 44. When the "Allow Apps to Request to Track" setting is turned off, or the privacy setting is engaged, Apple promises that 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" CAC ¶ 45. Apple promised that by turning off the "Share [Device] Analytics" setting, Plaintiffs and the Class could "disable the sharing of Device Analytics altogether," including "usage data." CAC ¶¶ 46, 107.

While Apple purports to provide users the choice as to whether Apple collects their data when users turn off "Allow Apps to Request to Track" and/or "Share [Device] Analytics" in their devices' privacy settings (CAC ¶ 49)—and even promises its users that it "respect[s] your ability to know, access, correct, transfer, restrict the processing of [...] your personal data," (CAC ¶ 48)—Apple does not honor such requests. CAC ¶¶ 50, 56. Unbeknownst to consumers, and in contradiction of Apple's privacy promises, Apple tracks and collects large swaths of personal information from mobile device users while they use the Apps, regardless of device users' opting out of settings that might otherwise permit the data sharing. This includes intimate details about individuals' lives, interests, app usage, app browsing communications, personal information, and information relating to the mobile device itself. CAC ¶¶ 4-6, 50. A recent study from security researchers at Mysk confirmed that the App Store harvests information about every single thing mobile device users do in real time, including what was tapped on, what software was searched for based on input of search terms, what ads were displayed, how long a page was viewed, and how the software was found. CAC ¶¶ 51-52. Stocks collects mobile device users' lists of watched stocks, the names of stocks viewed and searched for and time stamps when that occurred, as well as record of a news articles seen in the App. CAC ¶ 54. Apple also collects "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. CAC ¶ 55. As such, Apple tracks and collects detailed information about mobile device users while they use the Apps; Apple collects this information in contradiction of its own privacy promises; and the tracked and collected user data is directly linked to a mobile device user. CAC ¶ 56.

The enormous wealth of personal information and user data that Apple collects has substantial economic value. CAC ¶¶ 64-84. This data is a vast source of revenue for tech companies like Apple. CAC ¶¶ 60-64. But it may also reveal personal and confidential information, including

intimate personal facts and data that users, like Plaintiffs, do not want collected. CAC ¶¶ 11-25. Despite consumers expressly declining to give Apple permission to track and collect their data, Apple does just that by creating a detailed record of users' device use and habits and using that data for its own pecuniary gain. CAC ¶¶ 5, 284.

Plaintiffs were injured by Apple's conduct. CAC ¶¶ 118, 128, 137, 149, 233, 237, 250, 253, 270, 273. Plaintiffs are Apple mobile device users who sought to exercise control over their personal data by choosing certain settings that would restrict Apple's collection, storing and use of such data. CAC ¶¶ 11-25. Plaintiffs never consented to Apple tracking their confidential communications while "Allow Apps to Request to Track" and "Share iPhone Analytics" were turned off. CAC ¶¶ 11-25, 109, 114. Plaintiffs allege that Apple's conduct has needlessly harmed Plaintiffs and the Class by capturing a large swath of personally identifying information, including intimate personal facts and data in the form of their user data. CAC ¶ 146. Plaintiffs further allege that, given the monetary value of individual personal information, Apple deprived Plaintiffs and the Class of the economic value of their interactions with Apple's Apps, without providing proper consideration. CAC ¶ 147. In light of these well-pled allegations, Apple's motion to dismiss should be denied.

ARGUMENT

I. PLAINTIFFS ALLEGE SUFFICIENT FACTS TO CONFER STANDING

Apple contends that Plaintiffs insufficiently allege facts and legal theories surrounding its data collection and thus have "neither establish[ed] Article III standing nor state[d] a claim under Rules 8 or 9(b)." MTD at 8. But in the Ninth Circuit, consumers have standing when they allege violations of privacy statutes because "[v]iolations of the right to privacy have long been actionable at common law." *See In re Facebook, Inc., Internet Tracking Litigation*, 956 F.3d 589, 598 (9th Cir. 2020) ("*In re Facebook*"); *see also id.* ("A right to privacy encompasses the individual's control of information concerning his or her person" and CIPA and WESCA "codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing."); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) (same); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3d Cir. 2019) ("*In re Google II*") ("a concrete injury for Article III standing purposes occurs when Google, or any other third party, tracks

a person's internet browser activity without authorization."); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019); *Yockey v. Salesforce, Inc.*, 2023 WL 5519323, at *3 (N.D. Cal. Aug. 25, 2023); *Licea v. Cinmar, LLC*, 659 F. Supp. 3d 1096 (C.D. Cal. 2023); *Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072 (C.D. Cal. 2023). Here, Plaintiffs have so alleged.

The Ninth Circuit's recent decision in *Jones v. Ford Motor Co.*, 85 F.4th 570 (9th Cir. 2023), disposes of Apple's argument. In *Jones*, 85 F.4th at 573, the plaintiff alleged his "private communications were unlawfully recorded from [his] cellphone and permanently stored on his Ford vehicle in violation of the [Washington wiretapping statute]." The Ninth Circuit, noting that "the relevant law is settled[,]" held that these allegations sufficed for Article III standing. *See id.* at 574 ("At the pleading stage, those allegations plausibly articulate an Article III injury because they claim violation of a substantive privacy right."). Here, Plaintiffs' CAC contains extensive allegations about what data was collected. *See*, *e.g.*, CAC ¶¶ 52, 54-56. Plaintiffs allege the Apps that they regularly used. *See id.* ¶¶ 11-25 (detailing Plaintiff-specific allegations, including Apps "regularly used" by individual plaintiffs). Each Plaintiff alleges that "Apple accessed and recorded [their] data while […] using Apple's mobile applications." *See id.* And to the extent that Apple argues that Plaintiffs "do not explain why [alleged] collection of [their] data violates any law" (*see* MTD at 7), Plaintiffs have alleged *twelve* counts of illegal conduct on Apple's part, and explained each cause of action extensively. *See generally id* ¶¶ 100-287. No more is required.

Despite Apple's arguments (MTD at 8-9), "courts have rejected" the position that "Plaintiffs must plead the exact communications they had with the [Defendant]." *See James v. Walt Disney Co.*, 2023 WL 7392285, at *11 (N.D. Cal. Nov. 8, 2023); *see also Byars v. Goodyear Tire & Rubber Co.*, 654 F. Supp. 3d 1020 (C.D. Cal. 2023) (Finding "no requirement that Byars specifically allege the exact contents of her communications with Goodyear."). And whether the information intercepted was "sensitive enough" to constitute an injury is a premature factual question. *See, e.g.*, *Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 2838118, at *8 (N.D. Cal. Apr. 6, 2023) ("[D]eterminations of the egregiousness of the privacy intrusion are not usually resolved at the pleading stage."). Rather, a plaintiff "merely needs to show that the contents were not record information such as her name and address" *James*, 2023 WL 7392285, at *11 (quotation omitted). Plaintiffs have done so. *See* CAC ¶¶

52, 54-56.

Every decision cited by Apple on standing (1) predates *Jones* and (2) rested on the notion that no "sensitive," "personal," or "private" information was collected. *See Lightoller v. Jetblue Airways Corp.*, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023); *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023); *Cook v. GameStop, Inc.*, 2023 WL 5529772, at *4-5 (W.D. Pa. Aug. 28, 2023); *Mikulsky v. Noom, Inc.*, 2023 WL 4567096, at *4-5 (S.D. Cal. July 17, 2023); *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023); *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1188 (N.D. Cal. 2020); *Valenzuela v. Keurig Green Mountain, Inc.*, 2023 WL 6609351, at *3 (N.D. Cal. Oct. 10, 2023). But neither *Jones* nor *In re Facebook* nor the Third Circuit's *In re Google* opinions rested on the *nature* of the data collected; they rested on the fact that the data was collected *without consent*. Pertinently, *In re Facebook* and *In re Google I* and *II* involved basic browsing data: web pages and URLs that users visited. *See In re Facebook*, 956 F.3d at 596 (Information collected "included the website's Uniform Resource Locator ('URL') that was accessed by the user."); *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 135 (3d Cir. 2015) ("*In re Google I*") ("[P]laintiffs allege that the defendants acquired and tracked the URLs they visited…"). Plaintiffs' harm here does not depend on the nature of the data, but the fact that Apple tracked a person's usage activity without authorization, as well as in violation of its promises not to do so. *See In re Google II*, 934 F.3d at 325. Such conduct "interfere[s] with [P]laintiffs' control over their personal data," which "[n]umerous courts, including the Ninth Circuit, have found […] to be sufficient for standing on account of their injury implicating an invasion of the historically recognized right to privacy." *Leonard v. McMenamins, Inc.*, 2022 WL 4017674, at *5 (W.D. Wash. Sept. 2, 2022) (cleaned up).

As a final note, Apple also cites several cases to argue that Plaintiffs' factual allegations are too conclusory to state claims. MTD at 8-9. But Plaintiffs allege that their personal and sensitive data was collected (*see* CAC ¶¶ 11-25), and Apple does not deny that the collection occurred. That is sufficient for standing. *See supra*.

II. APPLE HAS NOT MET ITS BURDEN OF ESTABLISHING CONSENT

Consent to data collection "must be actual." *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1063 (N.D. Cal. 2021) (quoting *In re Google, Inc.*, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013)). "[F]or consent to be actual, the disclosures [relied on by the defendant] must 'explicitly notify' users of the practice at issue." *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021) (internal quotation omitted); *see also Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 847–48 (N.D. Cal. 2014) (to obtain consent, the disclosures must have given users notice of the "specific practice" at issue). For a finding of consent, "[t]he disclosures must have only one plausible interpretation." *Brown*, 525 F. Supp. 3d at 1063 (citing *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 794 (N.D. Cal. 2019)). As Judge Orrick observed, "consent to a fight with fists is not consent to an act of a very different character, such as biting off a finger, stabbing with a knife, or using brass knuckles." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 793 (N.D. Cal. 2022) (quoting Restatement (Second) of Torts § 892A (1979)). Courts examine "whether a reasonable user who viewed [Apple's] disclosures would have understood that [Apple] was collecting the information at issue." *Id.* (citing *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014)). Because consent is an affirmative defense, as the party seeking the benefit of the defense, Apple has the burden to show consent. *Id.* (citing *Calhoun*, 526 F. Supp. 3d at 620). "If a reasonable user could have plausibly interpreted the contract language as not disclosing that the defendant would engage in particular conduct, then the defendant cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent)." *Brown*, 525 F. Supp. 3d at 1063 (alterations omitted) (quoting *In re Facebook*, 402 F. Supp. 3d at 789-90).

Apple contends that Plaintiffs consented to Apple's data collection, pointing to several of its policies and written disclosures. First, it relies upon its software licenses for its operating systems, which are not a part of Plaintiffs' CAC. Apple contends that the licenses "provide[] transparency into what data is collected and how that data is used" because the licenses disclose that "certain features may require information from your Device." MTD at 2 (internal citations omitted). But as Apple admits, the specific practices of Apple's data collection are hidden as "details will be provided regarding what information is sent to Apple and how the information may be used" when the feature

is first used. *Id.* Critically, a core allegation of Plaintiffs' CAC is that they turned *off* various features, such as the "Share iPhone Analytics" option on their phone. *See*, *e.g.*, CAC ¶¶ 13-20, 24-25.

Both parties agree that the software licenses incorporate Apple's Privacy Policy. *See id*, ¶ 103; MTD at 10. But Apple's reliance on the Privacy Policy to support its consent defense, which is premature on a motion to dismiss, fails. Apple argues that the Privacy Policy discloses that Apple may collect the types of data Plaintiffs complain of here, and that because Plaintiffs continued to use apps after receiving such notice, "that constitutes consent to the collection under applicable law," thus foreclosing Plaintiffs' claims. MTD at 12. But even if the Privacy Policy can be read broadly to include the day-to-day *use* of the device, that language is modified by the provision in the Privacy Policy that states: "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." CAC ¶ 48 (emphasis added). In light of this language informing users they had the right to withdraw their consent to Apple's first-party processing of their personal data, it was not unreasonable for Plaintiffs to believe they, in fact, *did* withdraw their consent to Apple's data collection practices when they changed the "Share [Device] Analytics and/or Allow Apps to Request to Track" setting on their devices. CAC ¶¶ 11-25.

For the same reason, Apple's contention that various app launch screens gave notice that users' data "may be used to personalize your experience, send you notifications including for Apple marketing, improve the store, and prevent fraud" also fails. MTD at 3. Even if the welcome screens provided notice when users' data might be used and for what purpose, it again was not unreasonable for Plaintiffs to believe that they withdrew consent to have Apple collect and use their data when they turned off the controls above.

The ability to choose not to "[h]elp Apple improve its products and services by automatically sending diagnostics and usage data" also undercuts Apple's argument that service-specific disclosures gave Plaintiffs notice of the specific practices at issue. MTD at 4. A user who has chosen not to share her data to help "improve" Apple's products would reasonably believe her data was no longer being used for that purpose after switching off those controls. Even if Apple's product-specific disclosures, which are not before the Court at this time, give notice that Apple was collecting Plaintiffs' data at the instant of using an App, the disclosure does not put users on notice that users'

data is being shared *continuously* despite asserting privacy rights through users' settings. *See* CAC ¶¶ 44-56.

In sum, Apple points to policies and written notices in which it purports to disclose to users that their data was being collected, used, and shared and the purposes for which it was being collected, used, and shared. But it ignores its own representation to users that they "have the right to withdraw [their] consent at any time." CAC ¶ 48. The California Supreme Court has noted that "privacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic." *Sanders v. Am. Broad. Companies, Inc.*, 20 Cal.4th 907, 916, 978 P.2d 67 (Cal. 1999). Thus, "users can consent to some aspects of a defendant's conduct while not consenting to other aspects of a defendant's conduct." *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1076 (N.D. Cal. 2016). And consenting to a defendant's conduct or practices once or even multiple times does not mean that a plaintiff consents to the defendant's practices every time. *See id.*

Thus, Plaintiffs continuing to use their Apple devices and Apps after being put on notice of Apple's data collection practices does not mean that they continued to consent to those practices after they reasonably believed they had withdrawn their consent by turning off the data sharing controls. CAC ¶¶ 11-25. Apple argues that turning off the "Allow Apps to Request to Track" and/or "Share [Device] Analytics" settings are unrelated and do not alter Plaintiffs' consent. MTD at 12-14. But whether this is true and whether users could plausibly believe that these were the mechanisms for "withdraw[ing their] consent" to Apple's data collection "at any time" (CAC ¶ 48) are highly factual questions that are not capable of resolution at the motion to dismiss stage. *See Balanzar v. Fid. Brokerage Servs., LLC*, 654 F. Supp. 3d 1075, 1081 (S.D. Cal. 2023) ("The Court agrees with Plaintiff that the question of whether Fidelity received the statutorily required consent is a factual question not appropriate for resolution at the Motion to Dismiss stage."); *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 795 n.16 (N.D. Cal. 2019) (the issue of whether plaintiffs explicitly or impliedly consented to the defendant's challenged conduct in contractual language "cannot be resolved at the pleading stage in this case.").

At this stage, without the benefit of discovery, it cannot be said that Apple's disclosures "have only one plausible interpretation for a finding of consent." *Brown*, 525 F. Supp. 3d at 1063. Apple's arguments about consent therefore do not warrant dismissal of Plaintiffs' claims.

III. PLAINTIFFS ADEQUATELY ALLEGE BREACH OF CONTRACT

"The elements for a breach of contract claim are "'(1) the existence of the contract, (2) plaintiff's performance or excuse for nonperformance, (3) defendant's breach, and (4) the resulting damages to the plaintiff.'" *Parino v. BidRack, Inc.*, 838 F. Supp. 2d 900, 907–08 (N.D. Cal. 2011) quoting *Oasis W. Realty, LLC v. Goldman,* 51 Cal.4th 811, 821 (2011). Here, there is no dispute that the Privacy Policy and Family Disclosure are contracts nor is there any dispute – at this stage – that Plaintiffs (or their guardians) purchased Apple's devices, created accounts, changed their privacy settings to protect their data, and used Apple's Apps. *See* CAC ¶¶ 11-25, 103-114; *see also* MTD, at § III.A-B. Furthermore, the device's settings are incorporated by reference into the terms of the Privacy Policy. *Id.* at ¶103. Not only is the term "Settings" specifically referenced in the Privacy Policy, but consumers are directed to the "Settings" for additional information. CAC ¶¶ 44, 49, 103; *see In re Holl*, 925 F.3d 1076, 1084 (9th Cir. 2019) quoting *Shaw v. Regents of Univ. of Cal.*, 58 Cal. App. 4th 44, 54 (1997) (incorporations by reference are "valid [and binding] so long as the incorporation is 'clear and unequivocal, the reference [is] called to the attention of the other party and he [ ] consent[s] thereto, and the terms of the incorporated document [are] known or easily available'").

A. Plaintiffs Detailed Apple's Breach of the Parties' Express Contract

"The 'clear and explicit' meaning of contract terms, interpreted in their 'ordinary and popular sense,' governs judicial interpretation." *Westport Ins. Corp. v. N. California Relief*, 76 F. Supp. 3d 869, 879 (N.D. Cal. 2014) (citation omitted). Under California law, "[a] contract term will be considered ambiguous when it is capable of two or more constructions, both of which are reasonable." *RLI Ins. Co. v. City of Visalia*, 297 F. Supp. 3d 1038, 1049 (E.D. Cal. 2018), *aff'd*, 770 F. App'x 377 (9th Cir. 2019); *see Pac. Gas & Elec. Co. v. G. W. Thomas Drayage & Rigging Co.*, 69 Cal. 2d 33, 41, n.9 (1968) ("the double sense in which the word 'indemnify' is used in statutes and defined in dictionaries demonstrate the existence of an ambiguity."). Lastly, "ambiguous contract

provisions should be construed against the drafter." *Int'l Bhd. Of Teamsters v. NASA Servs., Inc.*, 957 F.3d 1038, 1042 (9th Cir. 2020).

Here, Plaintiffs allege that Apple breached the express contract formed between the parties based on Apple's explicit promises that:

- refusing to "Allow Apps to Request to Track" would ensure that "all apps […] will be blocked from accessing the device's Advertising Identifier[;]"
- disabling "Share [Device] Analytics" would prevent Defendant from "sending daily diagnostic and usage data[;]"and
- Apple would "not knowingly collect, use, or disclose any personal information from your child without your verifiable parental consent unless a COPPA exception applies."

CAC ¶¶ 32-49, 103-113.This means that Apple promised Plaintiffs and the Class Members that Apple would not collect ***any*** of their usage data, daily diagnostics, and advertising identifier(s) if consumers so requested. Additionally, for children, Apple promised not to collect, use, or disclose any personal information, including data, without permission.

Although Apple argues that the term "usage data" refers to "specific technical performance data," (MTD at 4) the ordinary and popular interpretation of the term "usage data" means any data created by the consumer's use of Apple's Apps that is collected by Apple, and the phrase "accessing the device's Advertising Identifier" to include when the same information is collected by Apple's Apps tracking users across third-party's applications and services. CAC ¶¶ 115, 122. Plaintiffs' reasonable interpretation of the phrase "usage data" is supported by the ordinary dictionary definitions of those words: *Usage*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/usage (last accessed Jan. 14, 2024) ("the action, amount, or mode of using"); *Data*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/data (last accessed Jan. 14, 2024) ("information in digital form that can be transmitted or processed"); *Usage Data definition*, LAW INSIDER, https://www.lawinsider.com/dictionary/usage-data (last accessed Jan. 14, 2024) ("**Usage Data** means data collected about the User's use of the Service. For example, how often the User accesses a to do list, or what photo(s) they favorite.") (original emphasis). Moreover, these

ordinary and popular dictionary definitions are consistent with Apple's own use and guidance of these terms. *See App privacy details on the App Store*, APPLE, https://developer.apple.com/app-store/app-privacy-details/ (last accessed Jan. 14, 2024) ("Usage Data[:] [1] Product Interaction [-] Such as app launches, taps, clicks, scrolling information, music listening data, video views, saved place in a game, video, or song, or other information about how the user interacts with the app[;] [2] Advertising Data [-] Such as information about the advertisements the user has seen[;] [3] Other Usage Data [-] Any other data about user activity in the app"); *App Store & Privacy*, APPLE, https://www.apple.com/legal/privacy/data/en/app-store/ (last accessed Jan. 14, 2024) ("app usage data stored on your device — such as the apps you frequently open, the time you spend using certain apps, and your app installs and uninstalls"); *Sensor & Usage Data & Privacy*, APPLE, https://www.apple.com/legal/privacy/data/en/sensor-usage-data/ (last accessed Jan. 14, 2024) ("Usage Data is information about how you use and interact with your iOS and watchOS devices and software. For example, this may include information about keyboard usage, the number of messages you send, the number of calls you make and receive, the categories of apps you use, the categories of websites you visit, when certain sensor and usage events are recorded, and when you wear your Apple Watch."); *About privacy information on the App Store and the choices you have to control your data*, APPLE, https://support.apple.com/en-us/102399 (last accessed Jan. 14, 2024) ("usage data such as app launches").

Accordingly, Plaintiffs have adequately put forth their reasonable interpretation of Apple's representations – Apple expressly promised to protect its customers' confidentiality concerning the data created from their usage of Apple's Apps, especially when specifically requested by Plaintiffs and Class Members through their privacy-related settings. *See In re Facebook Priv. Litig.*, 192 F. Supp. 3d 1053, 1058 (N.D. Cal. 2016) (finding plaintiffs sufficiently alleged defendant breached its promise to provide confidentiality); *In re Google, Inc. Privacy Pol'y Litig.*, 58 F. Supp. 3d 968, 989 (N.D. Cal. 2014) (same). To the extent that Apple may also provide a reasonable interpretation of the subject terms, the terms are rendered ambiguous and must be construed against the drafter, Apple. *Williams v. Apple, Inc.*, 449 F. Supp. 3d 892, 909 (N.D. Cal. 2020) ("Given the fact that Apple and Plaintiffs both provide reasonable interpretations, the disputed contractual language is ambiguous").

Likewise, even if Apple were correct that the term "Settings" as mentioned in the Privacy Policy actually refers to welcome screens and service-specific disclosures rather than the information contained in the "Settings related to those features" (CAC ¶ 103), that would render the Privacy Policy ambiguous and should be interpreted as Plaintiffs allege at this stage of the litigation. Regardless, the Parties' disagreement on the interpretation of the ambiguous contract is better resolved at a later stage in the proceedings. *See Bailey Venture Partners XVI, LLC v. Myall*, 2023 WL 3772026, at *4 (N.D. Cal. May 1, 2023) ("interpretation of ambiguous terms in a contract is a question of fact for the jury and is not appropriate at the motion to dismiss stage.").

Lastly, Apple contends that the Child Plaintiffs cannot "pursue contract claims based on Apple's Family Disclosure." MTD at 15. That is wrong. First, the Child Plaintiffs sufficiently allege a claim based on Apple's breach of its promise to get verifiable parental consent before collecting Child Plaintiffs' and the Minor Subclass Members' data. *See* CAC ¶¶ 111-113, 116-117. Second, Child Plaintiffs are both under the age of 13. Furthermore, it is a matter of interpretation – which cannot be resolved at this stage of the litigation – whether children over 13 being exempt from "Family Sharing" (defined as allowing users "to share purchases, subscriptions, and more with up to five other family members") (*Family Privacy Disclosure for Children*, APPLE, https://www.apple.com/legal/privacy/en-ww/parent-disclosure/ (last accessed Dec. 27, 2023)) ends Apple's promise to "not knowingly collect, use, or disclose any personal information from [a] child without […] verifiable parental consent." CAC ¶ 111; *see Tessera, Inc. v. UTAC (Taiwan) Corp.*, 2016 WL 8729937, at *6 (N.D. Cal. Jan. 15, 2016) (Davila, J.) ("arriving at the proper construction of the disputed [contractual] language will turn on the credibility of the extra-contractual evidence; an issue that only a jury can resolve."). The Child Plaintiffs' parents did not consent to Apple's collection of their children's data through Apple's Apps, including by not pressing "Continue" on each App's "Welcome Screen." *See* CAC ¶¶ 16, 24, 114, 116; *see also* Transcript of Bench Trial at 2473:1-11, *United States, et al. v. Google, LLC*, Case No. 1:20-CV-03010 (D.C. Sept. 6, 2023), *available at* https://thecapitolforum.com/wp-content/uploads/2023/10/Eddy-Cue-AM-Testimony_REDACTED_FINAL.pdf (Testimony of Defendant's Senior Vice President of Services: "Q [T]he first time a user opens the [Apple] maps app, are they given a choice about whether to

allow maps to use their location? A Yes, [the consent screens are] appropriate to ask at the time that they're using those applications. They're not appropriate to ask at another time."). Third, the Child Plaintiffs and Minor Subclass Members are third-party beneficiaries of the Family Disclosure. *See In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *19 (N.D. Cal. May 27, 2016) (finding plaintiff sufficiently stated a claim for breach as a third-party beneficiary of the privacy agreement); *see also Ferreira v. Uber Techs., Inc.*, 2023 WL 7284161, at *4 (N.D. Cal. Nov. 3, 2023) quoting *Ngo v. BMW of N. Am., LLC*, 23 F.4th 942, 946 (9th Cir. 2022) ("To qualify as a third-party beneficiary, the non-signatory is 'obligated to prove that 'express provisions of the contract,' considered in light of the 'relevant circumstances,' show that (1) 'the third party would in fact benefit from the contract;' (2) 'a motivating purpose of the contracting parties was to provide a benefit to the third party;' and (3) permitting the third party to enforce the contract 'is consistent with the objectives of the contract and the reasonable expectations of the contracting parties.'"). Even if the Child Plaintiffs were not third-party beneficiaries, which they are, their parents could easily take the Child Plaintiffs' place and the Minor Subclass definition could be modified similarly. Since Plaintiffs allege that Apple collected their data despite changing their privacy-related settings to prevent Apple from collecting their usage data, Plaintiffs sufficiently allege Apple breached the parties' express contract.

B. Plaintiffs Sufficiently Allege Apple Breached an Implied-in-Fact Contract and the Implied Covenant of Good Faith and Fair Dealing

"Courts routinely allow plaintiffs to plead both implied contract and express contract theories, as long as those theories are pled in the alternative." *California Spine & Neurosurgery Inst. v. United Healthcare Ins. Co.*, 2019 WL 4450842, at *4 (N.D. Cal. Sept. 17, 2019). The terms of the parties' implied contract can be determined through Apple's statements in various materials besides the software agreements as well as course of conduct. *See Arredondo v. Univ. of La Verne*, 618 F. Supp. 3d 937, 946 (C.D. Cal. 2022) ("Because a formal contract between a student and university is rarely prepared, the general nature and terms of the agreement are usually implied, with specific terms to be found in the university bulletin and other publications; customs and usages can also become specific terms by implications.") (internal citations omitted).

Here, Plaintiffs alternatively allege that Apple's marketing materials, public statements, license agreements, and privacy disclosures promise consumers confidentiality and Apple assures customers that it "builds privacy protections into its products and services." MTD at 1; *see* CAC ¶ 42. Specifically, Apple has stated in various marketing and disclosures:

- "Privacy. That's iPhone." often also including the web address of Apple's Privacy Policy;
- "We're in the business of staying out of yours.";
- "Privacy is King.";
- "Our apps mind their business. Not yours[;]" and
- "Whatever you choose is up to you…App Tracking Transparency. A simple new feature that puts your data back in your control."

CAC ¶¶ 32-49, 103-113. These additional statement and representations, combined with the express terms of the contract documents, form the basis of an implied-in-fact contract which Apple has breached. *See Doe v. Regents of Univ. of California*, 2023 WL 3316766, at *7 (N.D. Cal. May 8, 2023) (finding "the Notice of Privacy and Privacy Statement, providing assurances" were the basis for an implied contract).

Likewise, Plaintiffs properly allege their implied covenant of good faith and fair dealing claim because they allege that Apple unfairly withheld the benefit of privacy, as contracted between the parties, by using its discretion to collect data when Apple's customers requested – following the procedures set forth by Apple – that it refrain from such data collection. CAC ¶¶ 50-56, 134-135; *see In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 802 (N.D. Cal. 2019) (denying defendant's motion to dismiss the implied covenant claim where plaintiffs alleged "Facebook did nothing to enforce this [privacy] policy, thus giving users the impression that their [user] information was protected, while in reality countless app developers were using it for other purposes").

C. Plaintiffs Properly Allege Contract-Based Damages.

Unbeknownst to the average consumer (including Plaintiffs) until recently, Apple was breaking its promise by secretly collecting, maintaining, and using Plaintiffs and the Classes' data

via its Apps. CAC ¶¶ 50-56, 97-99. Apple engaged in this conduct despite the premium that Plaintiffs and Class Members paid for Apple's products. *Id. at* ¶¶ 118, 128, 137, 174, 209, 212, 232, 235, 249, 269; *see also* Kim Komando, *How the Google Pixel 8 stacks up against iPhone 15*, USA TODAY (Oct. 19, 2023, 5:23 ET), https://www.usatoday.com/story/tech/columnist/komando/2023/10/12/google-pixel-8-iphone-15-compared/71121711007/ (comparing phone prices: "$799 to $1,099 (iPhone [15]); $699 to $749 (Pixel [8])"). Not only did Plaintiffs and the Class Members pay a premium for their devices, but they also lost out on the monetary value of their data. CAC ¶¶ 57-84. That is sufficient to state damages for a breach of contract claim. *See Williams v. Apple, Inc.*, 338 F.R.D. 629, 652 (N.D. Cal. 2021) (finding a price premium is an appropriate measure of contractual damages); *In re Facebook Priv. Litig.*, 572 F. App'x 494 (9th Cir. 2014) ("dissemination of their personal information and by losing the sales value of that information […] are sufficient [allegations] to show the element of damages for [plaintiffs'] breach of contract and fraud claims."). Even if Plaintiffs did not suffer these actual damages, which they did, Plaintiffs would still be entitled to pursue nominal damages for Apple's conduct, which – as set forth above – resulted in a breach of contract. *See 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.").

Additionally, Plaintiffs are seeking injunctive relief and specific performance by having Apple no longer engage in the data collection, which are appropriate remedies for Apple's breach of contract. CAC at p. 54; *see Huawei Techs., Co. v. Samsung Elecs. Co.*, 2018 WL 1784065, at *9 (N.D. Cal. Apr. 13, 2018) (injunctive relief may be an appropriate remedy for breach of contract). Therefore, Plaintiffs sufficiently pled damages based on Apple's breach of contract.

IV. PLAINITFFS' PRIVACY CLAIMS SHOULD NOT BE DISMISSED.

A. Plaintiffs Adequately Allege Violation of CIPA

First, Apple contends Plaintiffs' CIPA claim must be dismissed because plaintiffs do not satisfy the 'without consent' element because all parties consented to the collection at issue." MTD at 17. As previously explained, *supra*, Section I, that argument is meritless. Second, Apple argues that dismissal is appropriate because mobile applications "do not qualify as an amplifying or

recording device." MTD at 18 (internal quotations omitted), but Apple applies the incorrect law and ignores that Plaintiffs' mobile phones are "recording device[s]" within the meaning of the statute.

Because "[a] claim under § 632 bears many similarities to a claim under the federal Wiretap Act," *see In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 827 (N.D. Cal. 2020), courts look to that statute "for guidance." *See People v. Roberts*, 184 Cal. App. 4th 1149, 1166 (2010). Indeed, for many elements, "[t]he analysis for a violation of CIPA is the same." *See, e.g.*, *Gonzales v. Uber Technologies, Inc.*, 305 F. Supp. 3d 1078, 1089 (N.D. Cal. 2018) (internal quotations omitted). And where the analysis differs, the Wiretap Act functions as "a floor, not a ceiling," because "a state wiretapping law can never be less restrictive than federal law." *see Villa v. Maricopa County*, 865 F.3d 1224, 1230 (9th Cir. 2017).

Under the Wiretap Act, courts routinely hold that "[s]oftware is a 'device.'" *See In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015); *see also United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wisc. 2019) (collecting cases). To be sure, the Wiretap Act regulates "electronic, mechanical, or other device[s]," *see* 18 U.S.C. § 2510(5), whereas CIPA regulates "electronic amplifying or recording device[s]." *See* Cal. Penal Code § 632(a). But that is a distinction without a difference. Where the statutes use different words to reach the same meaning, the analysis remains "the same." *See, e.g.*, *NovelPoster v. Javitch Canfield Group*, 140 F. Supp. 3d 938, 954 (N.D. Cal. 2014) (interpreting the term "interception"). To hold otherwise would construe CIPA narrower than the Wiretap Act, thereby defeating CIPA's purpose to cover "'new devices and techniques.'" *See In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 824–25 (N.D. Cal. 2020) (quoting Cal. Penal Code § 630). As such, because Apple "collect[ed] data through its proprietary Apps," *see* CAC ¶ 117, Apple intercepted their communications "by means of a 'device.'" *See Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1043 (N.D. Cal. 2014).

Apple points to *In re Google Location History Litigation*, but that decision is distinguishable. Authored by this Court, that case concerned section 637.7, which regulates "electronic tracking device[s]." *See In re Google Location History Litigation*, 428 F. Supp. 3d 185, 193 (N.D. Cal. 2019). As statutorily defined, those devices must "attach[] to a vehicle or other movable thing" and "reveal[] its location or movement by the transmission of electronic signals." *See* Cal. Penal Code § 637.7(d).

That language suggests the device must be tangible, "like a freestanding GPS unit hidden on a car." *See Heeger v. Facebook, Inc.*, 2019 WL 728477, at *3 (N.D. Cal. Dec. 27, 2019). By contrast, section 632 contains no such language, instead covering any device—tangible or not—that can "eavesdrop upon or record confidential communications." *See Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 689 (N.D. Cal. 2021) (quotations omitted). For that reason, "section 637.7 cases are distinguishable," and "software is a device under section 632(a)." *See Doe v. Meta Platforms, Inc.*, 2023 WL 5837443, at *7 (N.D. Cal. Sept. 7, 2023).

Even if software is not a device, Apple's argument fails. As alleged, "Apple's mobile devices […] are a 'device,'" *see* CAC ¶ 185, and Apple used those devices to "unlawfully intercept" Plaintiffs' communications "anytime they interact[ed] with an Apple app." *See id.* ¶ 150. Through those devices, moreover, "consumers expressly declin[ed] to give Apple permission to track and collect their data," *see id.* ¶ 5, yet Apple "collected, stored and used such data anyway." *See id.* ¶ 1. As a recent district court decision makes clear, those allegations are enough. *See Doe v. Microsoft Corp.*, 2023 WL 8780879, at *8 (W.D. Wash. Dec. 19, 2023) (upholding a CIPA claim where a defendant used both software and "receiving servers" to intercept communications, despite incorrectly holding that "software does not constitute a 'device'").

Apple next asserts that "plaintiffs have not adequately alleged that the data collected is a 'communication' within the meaning of CIPA." MTD at 18. But under any interpretation, Plaintiffs adequately allege that the collected information constitutes a "communication."

California courts interpret the term "communication" differently. On one end of the spectrum, "communication" is interpreted "broadly," covering "the exchange of thoughts, messages, or information by any means," *see People v. Gibbons*, 215 Cal. App. 3d 1204, 1208 (1989), including "conduct." *See People v. Lyon*, 61 Cal. App. 5th 237, 245 (2021); *see also Gonzales*, 305 F. Supp. 3d at 1086 (implying that "communication" includes "record information"). On the other end of the spectrum, "communication" only covers "content," not "the non-content-based content coincident to the communication." *See People v. Drennan*, 84 Cal. App. 4th 1349, 1357 (2000). Under either approach, Plaintiffs' allegations suffice.

Plaintiffs allege that, while browsing the mobile applications, Apple recorded what they "tapped on," what they "searched" through input of search terms, and what they "viewed." *See* CAC ¶ 52; *see also id.* ¶¶ 53–55. That information easily constitutes "content," revealing "the names of buttons clicked," *see In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 795 (N.D. Cal. 2022), along with "search queries" and "the particular document" requested. *See Brown v. Google LLC*, 2023 WL 5029899, at *15 (N.D. Cal. Aug. 7, 2023). Apple argues that "plaintiffs do not specify what actions they took in the app," *see* MTD at 18, but Plaintiffs identify the mobile applications they "regularly use[d]," *see* CAC ¶¶ 11–25, and those allegations are "enough to raise a right to relief above the speculative level." *See Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

Apple then contends that "collection of data that users provide to Apple is not akin to secretly 'recording' a confidential communication for later playback." MTD at 19. For support, Apple simply remarks that "[s]uch an expansive interpretation […] cannot be the law," leaving entirely unexplained how "recording" can mean anything but capturing communications. Apple cites two cases in support, but neither interprets "recording," so neither clarifies the point. *See In re Google Inc.*, 2013 WL 5423918, at *23 (addressing what constitutes "confidential"); *TBG Ins. Services Corp. v. Superior Court*, 96 Cal. 4th 443, 452 n.8 (2002) (addressing what establishes "consent"). Notwithstanding this, Apple collected Plaintiffs' communications "without consent" and "in real time," *see* CAC ¶¶ 52, 187, so under any reading, that conduct qualifies as "recording."

Apple ends by arguing that Plaintiffs fail to allege their communications were "confidential," reasoning that "no reasonable user would expect that their actions in Apple's apps would be private from Apple." MTD at 19. That argument not only ignores Plaintiffs' allegations, but it also runs head-first into well-established caselaw reviewing similar facts.

As explained by the California Supreme Court, communications are "confidential" if a party "had an objectively reasonable expectation that they were not being recorded." *Flanagan v. Falagan*, 27 Cal. 4th 766, 774 (2002). Plaintiffs meet that standard with ease. Through two settings, "Allow Apps to Request to Track" and "Share Analytics," Apple promised they "could control what data app developers can collect." CAC ¶ 44. By turning those settings off, developers are unable to access a panoply of information, like "system advertising identifier[s]," "performance statistics," "operating

system specifications," and how consumers "use [their] devices and applications." *Id.* at ¶¶ 45–47. Nowhere, not even in the fine print, did Apple ever disclose that, for its own mobile applications, it would continue collect user activity and identifiers "whether or not privacy settings were turned on or off." *Id.* ¶ 51. As multiple courts have held, similar representations created "an objectively reasonable expectation of privacy in this specific information." *See In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 800; *Brown*, 525 F. Supp. 3d at 1074 ("Google's policies did not indicate that data would be collected from users in private browsing mode and shared with Google."); *In re Facebook*, 956 F.3d at 603 (finding "a reasonable expectation of privacy" given "Facebook's affirmative statements that it would not receive information from third-party websites after users had logged out"). As such, Plaintiffs' communications were "confidential."

B. Plaintiffs Properly Allege Each Element of a WESCA Claim

While Pennsylvania has fashioned its Wiretapping and Electronic Surveillance Control Act ("WESCA") after the federal Electronic Communications Privacy Act, Pennsylvania has provided markedly greater protections to its citizens than provided by the federal Act. *Commonwealth v. Deck*, 954 A.2d 603, 607 (Pa. Super. Ct. 2008) ("Title III authorizes states to adopt wiretap statutes that trigger greater, but not lesser, protection that that available under federal law."). WESCA provides a private cause of action to "any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of [the Act] against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S.A. § 5725. It is a violation of WESCA to do any of the following:

> (1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication;
>
> (2) intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or
>
> (3) intentionally uses or endeavors to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know,

> that the information was obtained through the interception of a wire, electronic or oral communication.

18 Pa. C.S.A. § 5703. An "electronic communication" is defined broadly as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. C.S.A. § 5702. Not only is the unauthorized interception of communications illegal, "but also the disclosure and use of information obtained through such interceptions." *See Gelbard v. U.S.*, 408 U.S. 41, 52 (1972).

Additionally, WESCA requires consent from all parties. 18 Pa. C.S.A. § 5704(4) (it is not unlawful for "[a] person, to intercept a wire, electronic or oral communication, where ***all parties*** to the communication have given prior consent to such interception.") (emphasis added). Under established Pennsylvania law, a party to a communication may not intercept or record their own communications without the other party's consent. *See generally Commonwealth v. Deck*, 954 A.2d 603 (Pa. Super. Ct. 2008) (suppressing a recorded telephone call when one party had no knowledge of being recorded and did not consent). Here, as discussed above, Plaintiffs – including the PA Plaintiffs – did not consent to Apple's collection of their data. *See, supra,* Section II. Like in *Popa*, if Apple's argument that it can intercept the contents of Plaintiffs' communications because it is a "direct party," "the all-party consent requirement would disappear." *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 128 (3d Cir. 2022).

Apple makes much of the court's findings in *Commonwealth v. Proetto*, 771 A.2d 823, 831 (Pa. Super. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003) and *Commonwealth v. Cruttenden*, 58 A.3d 95, 98-100 (Pa. 2012) but ignores that WESCA was amended after the decisions were rendered. *See Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 127–28 (3d Cir. 2022) ("In adding [language to WESCA], the specific facts and holdings of *Proetto* and *Cruttenden*—exempting a law enforcement officer from liability for acquiring communications when he is an 'intended recipient' or is posing as one—are now explicitly included as a carve-out in the definition of 'intercept.' But this also limits the expansive reach of those cases.") (internal citations omitted). Furthermore, *Commonwealth v. Diego*, is easily distinguishable as the court found that the communication had ended before the

contents were shared, 2015 PA Super 143, 119 A.3d 370, 381 (2015), unlike here where the interception is occurring as consumers interact with Apple's Apps. *See* CAC ¶¶ 50-56, 187-189.

Recent decisions denying motions to dismiss WESCA claims demonstrate the sufficiency of Plaintiffs' allegations. For example, in *James v. Walt Disney Company*, Judge Chen found that the plaintiffs had adequately alleged the collection of the contents of their communications because "Plaintiffs have alleged that [the software] intercepted, *e.g.*, information about the webpages they viewed and searches they conducted. This makes it unlikely that Plaintiffs are simply implicating record information – *i.e.*, information regarding the characteristics of a message as opposed to the substance of the message itself." *James*, 2023 WL 7392285, at *11. Likewise, here, Plaintiffs allege that, after failing to get their consent, Apple collected "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," as well as "details about a user's mobile device." CAC ¶¶ 52, 186; *see* 18 Pa. C.S.A. § 5702 (contents defined as "*any information* concerning the substance, purport, or meaning of that communication.") (emphasis added); *In re Google I*, 806 F.3d at 137, 138 ("t]he line between contents and metadata is not abstract but contextual with respect to each communication" and "routing information and content are not mutually exclusive categories."). Accordingly, the Plaintiffs sufficiently allege that Apple intercepted more than just the collection of record information.

As another example, in *Oliver v. Noom, Inc.*, the court found that the session replay code on defendant's website was a device and denied the motion to dismiss. *Oliver v. Noom, Inc.*, 2023 WL 8600576, at *6 (W.D. Pa. Aug. 22, 2023) ("For a device to intercept an electronic communication, it usually must be embedded within (or connected to) the device on which the underlying communication is taking place."); *see Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 131 (3d Cir. 2022) (finding software code was the intercepting device); *see also Yockey*, 2023 WL 5519323, at *7 ("even if the communications at issue were sent directly through the Chat interface, Salesforce has nonetheless intercepted those communications within the meaning of WESCA to the extent that Salesforce received and stored those communications on its servers."). Here, Plaintiffs allege that their iPhones, iPads and/or Apple Watches are devices and the App software is rerouting their data

to Apple's server for storage, compilation, and use. CAC ¶¶ 169, 179, 185. Thus, Plaintiffs sufficiently allege that Apple intercepted their electronic communications using a device.

Therefore, Plaintiffs adequately allege that Apple violated WESCA.

C. Plaintiffs State a Claim for Invasion of Privacy

Apple states that to establish an invasion of privacy claim, "Plaintiffs must plead (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) a serious invasion of privacy constituting 'an egregious breach of . . . social norms.'" MTD at 22 (*citing Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35-37 (1994)). However, the 9th Circuit has framed the inquiry as "whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook*, 956 F.3d at 601. Contrary to Apple's assertions, case law in this District demonstrates that Plaintiffs' allegations meet either standard.

1. Plaintiffs Have a Legally Protected Privacy Interest

Apple argues that an "informational privacy interest is not adequately pleaded." MTD at 22. That is wrong. "California has recognized […] [an] interest[] in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy')." *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1232 (C.D. Cal. 2017) ("*In re Vizio*"). Courts have recognized that even the improper collection of URL information is legally protected. *In re Google I*, 806 F.3d at 151 ("California tort law treats as actionable an unwanted access to data by electronic or other covert means, in violation of the law or social norms.") (internal quotations omitted); *see also In re Vizio*, 238 F. Supp. 3d at 1232 ("[T]he Court rejects Vizio's argument that Plaintiffs have no cognizable interest in keeping detailed data about what video content they watch private."); *In re Facebook*, 956 F.3d at 603 ("In light of the privacy interests and Facebook's allegedly surreptitious and unseen data collection, Plaintiffs have adequately alleged a reasonable expectation of privacy.").

Apple also contends that Plaintiffs "do not establish that the information was disseminated or misused." MTD at 23. But that contradicts the pleadings, which allege that Apple made explicit representations that it would not collect the data at issue, and then not only surreptitiously collected the data anyways, but also monetized the data to Apple's benefit and Plaintiffs' detriment. CAC ¶¶ 1-6, 11-25, 32-56, 84, 141, 146-47, 149, 285. That constitutes "dissemination" and "misuse."

Apple also argues that a "reasonable consumer would understand that an app provider collects certain data from the app to provide and improve the requested services." MTD at 23. But that argument makes no sense in light of Plaintiffs' allegations that Apple collected and monetized data from Plaintiffs that Apple explicitly promised not to collect. *See, supra,* Section III. Additionally, that points to an issue of fact that is unripe at this stage of the proceedings. *Organic Consumers Ass'n v. Sanderson Farms, Inc.*, 284 F. Supp. 3d 1005, 1014 (N.D. Cal. 2018) ("Courts grant motions to dismiss under the reasonable consumer test only in rare situations in which the facts alleged in the complaint 'compel the conclusion as a matter of law that consumers are not likely to be deceived.'").

2. Plaintiffs Have a Reasonable Expectation of Privacy

Apple argues Plaintiffs had no reasonable expectation of privacy because Plaintiffs purportedly agreed to a "software license agreement when first using each app" and because Plaintiffs "cannot reasonably expect that data they knowingly provide to Apple would not be received by Apple." MTD at 23. Those arguments fly in the face of Plaintiffs' allegations and have been rejected by both the Ninth Circuit and courts in this district.

First, as stated above, Apple's software license agreement provides no shelter to Apple. *See supra*, Section II. Second, Apple's contentions that Plaintiffs cannot reasonably expect that Apple would not collect the data is nonsensical in light of the allegations that Apple asked Plaintiffs if they would like Apple to collect the data, Plaintiffs asked Apple not to, and then Apple collected the data anyway. CAC ¶¶ 1-6, 11-25, 32-56. Courts in this district have found near identical allegations sufficient to state a claim for invasion of privacy. *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078 (N.D. Cal. 2021) ("Plaintiffs in the instant case could have reasonably assumed that Google would not receive their data while they were in private browsing mode based on Google's representations."); *In re Facebook*, 956 F.3d at 602-03 ("Plaintiffs have plausibly alleged that, upon reading Facebook's statements in the applicable Data Use Policy, a user might assume that only logged-in user data would be collected. Plaintiffs have alleged that the applicable Help Center page affirmatively stated that logged-out user data would not be collected… the critical fact was that the online entity represented to the plaintiffs that their information would not be collected, but then proceeded to collect it anyway."); *Rodriguez v. Google LLC*, 2021 WL 2026726, at *8 (N.D. Cal.

May 21, 2021) (plaintiffs alleged "[the] interceptions took place after Google …. 'set an expectation' that it would not save plaintiffs' 'activity on ... apps ... that use Google services' unless plaintiffs turned WAA 'on.' … [i]n sum, the Ninth Circuit has left little doubt as to plaintiffs' intrusion upon seclusion and invasion of privacy claims. Both survive Google's motion to dismiss.") (*citing In re Facebook*, 956 F.3d at 602); *see also In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262, 293–94 (3d Cir. 2016) (holding, under analogous New Jersey law, that a reasonable expectation of privacy existed when Nickelodeon promised users that it would not collect information from website users, but then did anyways). Here, Plaintiffs' allegations regarding Apple's extensive representations about privacy and their allegations that Plaintiffs turned off "Allow Apps to Request to Track" and/or "Share [Device] Analytics" on their privacy controls meet this standard. CAC ¶¶ 1-6, 11-25, 32-56.

3. Apple Committed a Serious Invasion of Privacy

Apple argues that Plaintiffs do not state a claim for an invasion of privacy because Plaintiffs do not allege why the information that was collected was "sensitive." MTD at 24. That is wrong. Notably, Plaintiffs allege that Apple surreptitiously collected electronic communications after making explicit representations that is (CAC ¶¶ 1-6, 11-25, 32-56), and "courts have held that 'deceit can be a kind of 'plus' factor [that is] significant in ... making a privacy intrusion especially offensive.'" *In re Google Location Hist. Litig.*, 514 F. Supp. 3d 1147 (N.D. Cal. 2021) (internal quotations omitted); *Brown v. Google LLC*, 525 F. Supp. 3d at 1079 ("Moreover, as explained above, Google's representations regarding private browsing mode could have led users to assume that Google would not view their activity while in private browsing mode.").

Ultimately, whether Apple's conduct was sufficiently offensive raises a question of fact. *See In re Google Location History Litig.*, 514 F. Supp. 3d 1147 ("Whether Google's collection and storage of location data when Location History was set to off was highly offensive to a reasonable person is a question of fact."). On that basis, the Ninth Circuit reversed the dismissal of an invasion of privacy claim where Facebook only obtained internet history—which is far less than the scope of information obtained here. *See In re Facebook*, 956 F.3d at 606 ("The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage."); *Rodriguez*, 2021 WL 2026726, at *8 ("Nor is the

offensiveness of Google's putative misconduct any less a matter of 'public policy,' or any more susceptible to 'resol[ution] at the pleading stage,' than that ascribed to Facebook.") (*citing In re Facebook*, 956 F.3d at 602); *see also Moosejaw*, 2019 WL 5485330, at *3 (denying motion to dismiss because whether conduct is offensive is a factual question); *Opperman II*, 205 F. Supp. 3d at 1079 (same). Thus, Apple asks the Court to make the same reversible error made in *In re Facebook*.

Apple partially relies on *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986 (2011), but *Foglestrom* does not support Apple's position. As Judge Tigar explained in *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014) ("*Opperman I*"), *Folgelstrom* is "distinguishable" because it did not involve the "surreptitious" acquisition of personal information. Judge Tigar likewise rejected the argument that secretly acquiring personal information—like Apple has done here—is "routine commercial behavior," and concluded that whether the conduct at issue was "highly offensive" was a factual dispute "best left for a jury." *Opperman I*, 87 F. Supp. 3d at 1061; *see also In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d at 797 ("Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is."). Judge Tigar also declined to follow *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012), explaining he was "not persuaded by cases that have mechanically applied *Folgelstrom* to invasion of privacy claims." *Opperman II*, 205 F. Supp. 3d at 1078-79 (emphasis added). This Court should do the same.

V. PLAINTIFFS' CONSUMER PROTECTION CLAIMS SHOULD NOT BE DISMISSED

Plaintiffs' state law claims have similar elements – generally, requiring a plaintiff to plead unlawful or misleading conduct, damages, and a relationship between defendant's conduct and the injury. *See e.g., Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1069 (N.D. Cal. 2022) ("To plausibly allege a [...] UCL claim, a plaintiff must allege that they relied on a misrepresentation and suffered injury as a result."); *In re Anthem, Inc. v. Data Breach Litig.*, 162 F. Supp. 3d 953, 991 (N.D. Cal. 2016) (quoting *Orlander v. Staples, Inc.*, 802 F.3d 289, 300 (2d Cir. 2015) (Under NY GBL §§ 349 and 350, "a plaintiff must allege that a defendant has engaged in (1) consumer-oriented

conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice."); *Munning v. Gap, Inc.*, 238 F. Supp. 3d 1195, 1200 (N.D. Cal. 2017) (citing *Int'l Union of Operating Eng'rs Local No. 68 Welfare Fund v. Merck & Co.*, 192 N.J. 372, 389 (N.J. 2007) ("To state a valid NJCFA claim, a plaintiff must allege sufficient facts to demonstrate: (1) unlawful conduct; (2) an ascertainable loss; and (3) a causal relationship between the defendant's unlawful conduct and plaintiff's ascertainable loss."); *Blankship v. Pushpin Holdings, LLC*, 157 F. Supp. 3d 788, 792 (N.D. Ill. 2016) (An Illinois Consumer Fraud Act claim requires: "(1) a deceptive act or unfair practice occurred, (2) the defendant intended for plaintiff to rely on the deception, (3) the deception occurred in the course of conduct involving trade or commerce, (4) the plaintiff sustained actual damages, and (5) the damages were proximately caused by the defendant's deception."). Plaintiffs adequately allege the elements for their respective state law claims.

A. Plaintiffs Allege Apple Acted Deceptively and Unlawfully

Plaintiffs plainly allege that Apple's false misrepresentations, both about its commitment to privacy and the safety of user's data after selecting certain security settings, induced them to both purchase Apple's devices and use Apple Apps when they might not have otherwise. CAC ¶¶ 165(d-e), 167, 169, 171. The CAC identifies specific statements made by Apple, which are directed to consumers, assuring users that when they disable the "Allow Apps to Request to Track" setting, applications would not have the ability to access identifiers used to track users and or be "permitted to track" users' activities using other identifiers like an email address. *Id. at* ¶ 45. Apple also promises on its Legal page on "Device Analytics & Privacy" that turning off the "Share [Device] Analytics" setting would "disable the sharing of Device Analytics," which may "include [...] data about how you use your devices and applications." *Id.* at ¶ 46-47. On Plaintiffs' devices, the disclosure corresponding to the "Allow Apps to Request to Track" setting states that "[w]hen you disable Allow Apps to Request to Track, any app that attempts to ask you for your permission will be blocked from asking" and "all apps, other than those that you have previously given permission to track, will be blocked from accessing the device's Advertising Identifier." *Id. at* ¶ 106.

The CAC also clearly describes Apple's systematic, uniformly themed disclosure and marketing campaign based on Apple's seven-year global advertising campaign was pervasive and represented to customers that Apple values the privacy of its users and allows users to control who accesses and uses their data. *Id. at* ¶¶ 32-49. Further, the misrepresentations in the advertisements were all similarly focused on protecting and promoting the privacy of the users of Apple's devices, with some going further to say that the user would have control over their data privacy. *Id. at* ¶¶ 32-34, 36-43. Additionally, Plaintiffs allege that Apple was obliged to disclose this collection because it had exclusive knowledge that regardless of the setting, Apple collected and was in a "superior position to know" about how it used and exploited user data. *Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 926 (N.D. Cal. 2012).

Accordingly, Plaintiffs adequately allege this element of their state law claims. *See e.g.*, *Yastrab v. Apple Inc.*, 173 F. Supp. 3d 972, 980 (N.D. Cal. 2016) (citing *In re Tobacco II Cases*, 207 P.3d 20, 41 (Cal. 2009) (Under the CA UCL, "once the details of the campaign are particularly pled, individual reliance on the specific statements need not be."); *Williams v. Gerber Prod. Co.*, 552 F.3d 934, 938 (9th Cir. 2008) (quoting *Kasky v. Nike, Inc.*, 27 Cal. 4th 939, 951 (Cal. 2002) (The California Supreme Court interprets the UCL as prohibiting statements that "although true, [are] either actually misleading or [...] has a capacity, likelihood or tendency to deceive or confuse the public namely, a 'reasonable consumer.'"); *Johnson v. Nissan N. Am., Inc.*, 272 F. Supp. 3d 1168, 1184 (N.D. Cal. 2017) (quoting *Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A.*, 85 N.Y.2d 20, 25 (N.Y. Ct. App. 1995) ("An act is 'consumer oriented' when 'the acts or practices have a broader impact on consumers at large.'"); *Stutman v. Chem. Bank*, 95 N.Y.2d 24, 29 (2000) (reliance is not an element of the GBL claims, and plaintiffs only need show that a "material deceptive act" caused the injury); *Chow v. Aegis Mortg. Corp.*, 286 F.Supp.2d 956, 963,1018 (N.D. Ill. 2003) ("[P]laintiff need not show that defendant intended to deceive the plaintiff, but only that the defendant intended the plaintiff to rely on the (intentionally *or* unintentionally) deceptive information given.").

B. Plaintiffs Were Harmed by Apple's Conduct

As set forth above, Apple's assertions misled Plaintiffs into believing they could prevent Apple from tracking and collecting their information and data by turning off various settings. In reliance on this misrepresentation, Plaintiffs continued to use Apple Apps and subsequently suffered harm in the form of the loss of the economic value of their user data without the proper consideration. CAC ¶ 84. Plaintiffs also allege that had they "known of Apple's intention to collect and monetize their private information, [they] would not have purchased Apple's devices and/or used Apple's Apps," (*Id. at* ¶ 208), or paid a "premium price to other equivalent phones" for Apple's devices. *Id. at* ¶ 209. This is enough to satisfy the requirements at the pleading stage. *See e.g.*, *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 995 (N.D. Cal. 2016) (finding that "'Loss of Value of PII' constitute[d] a cognizable injury under GBL § 349); *Forcellati v. Hyland's, Inc.*, 876 F. Supp. 2d 1155, 1168-69 (C.D. Cal. 2012) (holding that plaintiff who alleged he "paid a price premium" due to the misrepresentations of the defendant had "sufficiently plead[] an ascertainably loss under the out-of-pocket theory"); *Bosland v. Warnock Dodge, Inc.*, 964 A.2d 741, 750 (N.J. 2009) ("[P]laintiff was the victim of an overcharge. More to the point, the overcharge in question is one that can be readily quantified and thus is ascertainable within the meaning of the CFA.")

C. Plaintiffs Plead Their Fraud-Based Claims with Particularity

Fed. R. Civ. P. 9(b) requires that claims sounding in fraud must state the claim with particularity and Plaintiffs can satisfy this heightened pleading standard by alleging the "who, what, when, where, and how" of their claim. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103 (9th Cir. 2003). In accordance with Rule 9(b), Plaintiffs plead their state consumer protection claims with sufficient particularity to provide the requisite notice to Apple. Apple (the, "who") (CAC ¶ 1); made statements and omissions regarding users' control over the privacy settings on their Apple devices and whether certain security options would allow Apple Apps to collect and profit off of users' data (the, "what") (*see, e.g.*, *Id. at* ¶ 4); through a concerted advertising campaign and representations and omissions made on its devices, website and, in its policies (the, "where") (*see e.g.*, *Id. at* ¶¶ 39, 44-47); before Plaintiffs purchased their devices and/or opted to use Apple Apps (the, "when") (*see, e.g.*, *Id. at* ¶¶ 12); and, thereby, inducing Plaintiffs to continue using Apple Apps based on the

representation that Apple Apps would not collect their data (the, "how") (*see, e.g.*, *Id. at* ¶¶ 208-09). In recognition of the particularity of Plaintiffs' allegations, Apple does not contend that Plaintiffs' state consumer protection claims do not provide it with the requisite notice to defend itself – in a seeming admission that the issue is not currently ripe for consideration. *See Kang v. P.F. Chang's China Bistro, Inc.*, 844 F. App'x 969, 970–71 (9th Cir. 2021) ("[D]etermining whether reasonable consumers are likely to be deceived will usually be a question of fact not appropriate for decision on a motion to dismiss.") (internal quotation omitted); *Bowring v. Sapporo U.S.A., Inc.*, 234 F. Supp. 3d 386, 390 (E.D.N.Y. 2017) ("Th[e] reasonable consumer inquiry is factual and in most instances, not resolved at the motion to dismiss stage."); *Akers v. Costco Wholesale Corp.*, 631 F. Supp. 3d 625, 631 (S.D. Ill. 2022) ("Frequently, ICFA claims involve disputed questions of fact not suitable for dismissal at the pleading stage[.]"). Therefore, Plaintiffs adequately allege their state law claims.

VI. PLAINTIFFS MAY PURSUE EQUITABLE CLAIMS IN THE ALTERNATIVE

Apple cites *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020), for the proposition that Plaintiffs' equitable claims should be dismissed because "the complaint seeks the legal remedy of damages under CIPA, WESCA, and GBL." MTD at 30. But that is not the law. In fact, the "majority of courts in this district" have held that *Sonner* does not require dismissal of equitable claims at the pleading stage. *See In re Natera Prenatal Testing Litig.*, 664 F. Supp. 3d 995 (N.D. Cal. 2023) (collecting cases); *see also Yeomans v. World Fin. Grp. Ins. Agency, Inc.*, 2022 WL 844152, at *7-8 (N.D. Cal. Mar. 22, 2022) (*Sonner* did not prevent plaintiffs from seeking restitution in the alternative to legal claims at the pleading stage). Plaintiffs here plead that they lack an adequate remedy at law. CAC ¶ 287. That is sufficient at this stage of the litigation. *See Moyle v. Liberty Mut. Retirement Ben. Plan.*, 823 F.3d 948, 962 (9th Cir. 2016) (permitting a plaintiff to pursue both legal and equitable relief).

VII. ALTERNATIVELY, PLAINTIFFS REQUEST LEAVE TO AMEND

Here, should the Court decide to grant Apple's motion – which it should not, Plaintiffs' respectfully request leave to amend. *See Smith, et al., v. Santa Cruz County, et al.*, 2023 WL 8360054, at *6 (N.D. Cal. Dec. 1, 2023) (J. Davila) (granting leave to amend). Plaintiffs can easily add additional information about the types/categories of data collected, the confidentiality of that data,

and which Apps were used by the Child Plaintiffs. Further, Plaintiffs have also recently discovered evidence that Apple is selling, or at the very least sharing, consumer' data – including minors' data – to foreign entities. *Letter to Hon. Merrick B. Garland*, RON WYDEN U.S. SENATOR FOR OREGON (Dec. 6, 2023), https://www.wyden.senate.gov/imo/media/doc/wyden_smartphone_push_notification_surveillance_letter.pdf ("The data [Apple] receive[s] includes metadata, detailing which app received a notification and when, as well as the phone and associated Apple […] account to which that notification was intended to be delivered. In certain instances, [Apple] might also receive unencrypted content, which could range from backend directives for the app to the actual text displayed to a user in an app notification."). Apple has admitted that it failed to disclose the collection and distribution of this data. Raphael Satter, *Governments Spying on Apple, Google users through push notifications – US senator*, REUTERS (Dec. 6, 2023), https://www.reuters.com/technology/cybersecurity/governments-spying-apple-google-users-through-push-notifications-us-senator-2023-12-06/. Additionally, recent research has revealed that third party applications of iPhones are able to secretly harvest user data and identifying information through application notifications, even when users turn off sharing of device analytics settings on the device. Thomas Germain, *iPhone Apps Secretly Harvest Data When They Send Your Notifications, Researchers Find*, GIZMODO (Jan. 25, 2024), https://gizmodo.com/iphone-apps-can-harvest-data-from-notifications-1851194537. To the extent the Court is inclined to grant the motion to dismiss, the Court should grant leave to amend.

CONCLUSION

Plaintiffs respectfully request that the Court deny Apple's Motion to Dismiss.

Dated: January 26, 2024

BURSOR & FISHER, P.A.

By: */s/ L. Timothy Fisher*
L. Timothy Fisher

L. Timothy Fisher (SBN 191626)
Brittany S. Scott (SBN 327132).
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com
bscott@bursor.com

BURSOR & FISHER, P.A.
Philip L. Fraietta*
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

LYNCH CARPENTER, LLP
(Eddie) Jae K. Kim (SBN 236805)
ekim@lcllp.com
Tiffine E. Malamphy (SBN 312239)
tiffine@lcllp.com
117 East Colorado Blvd., Suite 600
Pasadena, CA 91105
Telephone: (626) 550-1250
Facsimile: (619) 756-6991

LYNCH CARPENTER, LLP
Gary F. Lynch*
1133 Penn Avenue
Pittsburgh, PA 15232
Tel: (412) 322-9243
Fax: (412) 231-0246
gary@lcllp.com

**admitted pro hac vice*

Interim Co-Lead Counsel