Emily Johnson Henn (Bar No. 269482)
Kathryn E. Cahoy (Bar No. 298777)
COVINGTON & BURLING LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306-2112
Telephone: (650) 632-4700
Facsimile: (650) 632-4800
Email: ehenn@cov.com
Email: kcahoy@cov.com

Amy S. Heath (Bar No. 312516)
COVINGTON & BURLING LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
Telephone: (415) 591-7030
Facsimile: (415) 955-6530
Email: aheath@cov.com

Attorneys for Defendant Apple Inc.

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE APPLE DATA PRIVACY LITIGATION

Civil Case No.: 5:22-CV-07069-EJD

DEFENDANT'S NOTICE OF MOTION AND MOTION TO DISMISS CONSOLIDATED COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

NOTICE OF MOTION/MOTION: PLEASE TAKE NOTICE that on March 21, 2024, at 9:00 a.m., Apple will and hereby does move under F.R.C.P. 9(b), 12(b)(1), and 12(b)(6) to dismiss the consolidated class action complaint. The motion is based on the memorandum, documents incorporated by reference or judicially noticeable, and evidence and argument as the Court permits.

MEMORANDUM IN SUPPORT: INTRODUCTION AND STATEMENT OF ISSUES

Last November, two app developers at the software company Mysk tweeted that certain data was collected by the App Store, Music, TV, Books, and Stocks apps after they turned off the Share iPhone Analytics setting.[1] Based on the Mysk tweets, plaintiffs soon filed multiple lawsuits accusing Apple of invading their privacy and violating state wiretap laws. More than one year later, the consolidated class action complaint ("complaint") adds little to the Mysk tweets. And plaintiffs do not allege any facts about what data they believe was collected *from them*. Barebones allegations that plaintiffs used Apple apps and had unspecified data collected are insufficient to establish Article III standing or to state claims.

The claims also cannot withstand Apple's thorough and repeated disclosure of the collection Mysk highlighted. Apple believes privacy is a fundamental human right and builds privacy protections into its products and services. When it collects personal data, it discloses this collection to users. Apple presents these disclosures at various points, including during device setup and when the app is first opened. Plaintiffs do not contend that Apple breached the terms of any disclosure. Instead, they claim they thought that turning off the Share [Device] Analytics setting and another unrelated setting, called Allow Apps to Request to Track, would turn off *all* data collection from these apps.

Plaintiffs' theory is facially implausible. Many of the apps they focus on provide media services, which need certain data to deliver the songs, shows, and books that users purchase, personalize the services, and fight fraud—as the disclosures repeatedly explain. Moreover, the descriptions of the two settings make clear that they do not govern the data collection plaintiffs challenge here. Allow Apps to Request to Track lets users choose whether apps can ask permission to track them across apps or websites owned by other companies—it does not affect data collection in first-party apps that is not used to track users across other companies' sites. And Share [Device] Analytics concerns collection of technical performance data, such as data about app crashes or file compression effectiveness. Apple disclosed the

[1] Apple refers in this motion to that setting on iPhone, iPad, and Watch as "Share [Device] Analytics."

effect of these settings to users, including on the screens where plaintiffs could turn the settings on or off.

Each claim also suffers from other deficiencies. Plaintiffs do not allege actionable damages, which forecloses their contract and consumer-protection claims. They cannot base wiretap and privacy claims on the disclosed collection of data that Apple uses to provide requested services, and plaintiffs do not adequately allege any element of their wiretap claims. The consumer-protection claims do not satisfy Rule 9(b), and the Court lacks equitable jurisdiction to hear the Unfair Competition Law and unjust enrichment claims. For these reasons, among others, the complaint should be dismissed with prejudice.

STATEMENT OF FACTS

A. Apple Privacy Disclosures and App Data Collection.

From the moment a user sets up their device, Apple provides transparency into what data is collected and how that data is used. Contrary to plaintiffs' allegation that Apple's apps "secretly" collect data, Compl. ¶ 50, Apple notifies users of collection at multiple points, including in the devices' software license agreements presented during device setup, through the Privacy Policy, and as part of a "welcome screen" when the user first opens an app that collects personal data. Those welcome screens link to a detailed service-specific privacy disclosure tailored to the app, which is available on the device and online.

Software License Agreement. As part of a device's setup process, users agree to a software license. *See* Request for Judicial Notice ("RJN") Ex. 1 (iOS/iPad 16 Software License) at 1; Ex. 2 (watchOS Software License) at 1; *see also* Compl. ¶ 103 (citing license).[2] In a section titled "Consent to Use of Data," the licenses explain that certain features "may require information from your Device to provide their respective functions." It goes on, "When you turn on or use these features, details will be provided regarding what information is sent to Apple and how the information may be used." RJN Ex. 1 (iOS/iPad OS Software License) at 4; Ex. 2 (watchOS Software License) at 4. The software licenses incorporate Apple's Privacy Policy, discussed below. *See id.*

Privacy Policy. Apple's Privacy Policy discloses that Apple may collect account, device, contact, and transaction data, including "[y]our Apple ID and related account details" and "[d]ata from which your device could be identified." RJN Ex. 3 (Privacy Policy) at 3. It explains that Apple may collect "[d]ata

[2] Apple has concurrently filed a request for judicial notice and incorporation by reference.

about your activity on and use of our offerings, such as app launches within our services, including browsing history; search history; product interaction; crash data, performance and other diagnostic data; and other usage data." *Id.* Apple uses the collected data to "power [its] services, to process your transactions," and "for security and fraud prevention," among other uses. *Id.* at 4. "For example, if you would like to access a song through an Apple Music subscription, [Apple] collect[s] data on what songs you play in order to provide you with the content requested and for royalty purposes." *Id.* at 5.

For certain apps that collect personal data, the Privacy Policy explains that additional service-specific disclosures are presented to users in a welcome screen the first time a user opens that app and also are accessible through the app's settings and online: "[W]e provide data and privacy information embedded in our products and certain features that ask to use your personal data." *Id.* at 1. "You will be given an opportunity to review this product-specific information before using these features. You also can view this information at any time, either in settings related to those features and/or online at apple.com/legal/privacy/data." *Id.*; *see also id.* at 3 ("Descriptions of how Apple handles personal data for certain individual services are available at apple.com/legal/privacy/data.").

Welcome Screens. The first time a user opens an Apple app that collects personal data, a welcome screen provides key information about the app's data collection and use practices. For example, the App Store welcome screen states, "Your searches, browsing, purchases, and device trust score may be used to personalize your experience, send you notifications including for Apple marketing, improve the store, and prevent fraud." *See* RJN Ex. 4 (App Store welcome screen). A hyperlink leads to a longer disclosure, which is also available online and in the device's settings. *Id.* Users must click a "continue" button below the privacy summary before using the app. *Id.*; *see also* RJN Exs. 5-8 (other apps' welcome screens).

Service-Specific Disclosures. When an app collects personal information, a service-specific disclosure details the app's collection and use practices. Those disclosures are available (1) by clicking the hyperlink on the welcome screen, (2) on the device, by navigating to Settings > [App Name], and (3) online at https://www.apple.com/legal/privacy/data/. For example, the App Store & Privacy disclosure explains that, among other purposes, Apple "collect[s] your personal data so that we can provide you the content you purchase, download, or want to update in the App Store." RJN Ex. 9 (App Store & Privacy) at 1. It continues, "[t]o find ways to improve the stores, we use information about your browsing,

purchases, searches, and downloads. These records may be stored with IP address, a random unique identifier (where that arises), and Apple ID when you are signed in to . . . Apple online stores." *Id.*

The other service-specific disclosures are similar. They explain, among other things, that "Apple collects information about what you purchase and what you're watching in the Apple TV app . . . so [it] can display what you're watching across your supported devices." *See* RJN Ex. 11 (Apple TV App & Privacy) at 1. Music "collect[s] information about the songs and videos . . . you play or add to your music library" to customize recommendations and pay royalties. *See* RJN Ex. 10 (Apple Music & Privacy) at 3. And Apple Books collects device type and the amount of free space on your device "to assess whether requested content can be downloaded." *See* RJN Ex. 12 (Apple Books & Privacy) at 2.

B. Device Analytics Data and the Share [Device] Analytics Setting.

Entirely separate from the collection described in the service-specific disclosures, users can choose at the operating-system level whether to share with Apple certain "Device Analytics" data. Apple discloses that Device Analytics "may include details about hardware and operating system specifications, performance statistics, and data about how you use your devices and applications." *See* RJN Ex. 14 (Device Analytics & Privacy) at 1; Compl. ¶ 47. Users decide whether to share Device Analytics data as part of the device setup process and can change that choice at any time through the Share [Device] Analytics setting on the Analytics & Improvements page, located at Settings > Privacy & Security > Analytics & Improvements. *See* Compl. ¶ 107; RJN Ex. 15 (Share [Device] Analytics setting screen).

Below the setting, the following statement appears: "Help Apple improve its products and services by automatically sending daily diagnostic and usage data." *See* RJN Ex. 15 (Share [Device] Analytics setting screen); Compl. ¶ 107. A hyperlink providing more information follows, and that hyperlink takes users to a Device Analytics & Privacy disclosure. The disclosure explains that Device Analytics data includes specific technical performance data. *See* RJN Ex. 14 (Device Analytics & Privacy) at 1; Compl. ¶ 108. It then tells users how to view examples of Device Analytics: "You can review this information on your iOS device by going to Settings > Privacy & Security > Analytics & Improvements and tapping Analytics Data." *See* RJN Ex. 14 (Device Analytics & Privacy) at 1. The disclosure also explains that toggling Share [Device] Analytics off "disable[s] the sharing" of this data. *See id.*; Compl. ¶ 46. Nowhere does Apple represent that the Share [Device] Analytics setting affects the data collection detailed in the

service-specific disclosures, let alone all data collection in the apps. *See* Compl. ¶¶ 110, 117.

C. The Allow Apps to Request to Track Setting.

Apple also lets users choose whether apps can request to track their activity across apps and websites owned by other companies through the Allow Apps to Request to Track setting, located at Settings > Privacy & Security > Tracking. Compl. ¶¶ 44-45, 104-06. This setting only applies when an app wants to track a user across apps or websites owned by other companies. Even then, the setting controls only whether such an app can ask user permission to track; it does not, and does not purport to, turn off all data collection through a company's own apps.

Apple's setting descriptions and disclosures consistently explain its function. Directly below the setting, it says: "Allow apps *to ask* to track your activity across *other companies' apps and websites*. When this is off, all new app tracking requests are automatically denied." *See* RJN Ex. 16 (Allow Apps to Request to Track setting screen) (emphasis added). A hyperlink leads to a Tracking disclosure with more detail: "Apple requires app developers to *ask for permission* before they track your activity *across apps or websites they don't own*[.]" *See* RJN Ex. 17 (Tracking disclosure) at 1 (emphasis added); Compl. ¶¶ 105-06. It goes on: "You can control whether apps can ask for permission to track your activity . . . If you don't want to be asked for your permission, or do not want apps to access your device's Advertising Identifier, you can disable Allow Apps to Request to Track." RJN Ex. 17 (Tracking disclosure) at 3. Similarly, the Privacy Policy explains, "If you disable Allow Apps to Request to Track, third-party apps cannot request to use the Advertising Identifier . . . to track you across apps and websites *owned by other companies*." *See* RJN Ex. 3 (Privacy Policy) at 8 (emphasis added).

D. Parental Consent for Children Under the Age of 13.

Apple does not permit children under the age of 13 to create their own Apple IDs. *See* RJN Ex. 18 (Family Privacy Disclosure for Children ("Family Disclosure")) at 3. Instead, a parent or guardian must create the account, as explained in the Family Disclosure and the incorporated Privacy Policy. *See id.*; Ex. 3 (Privacy Policy) at 7. During the setup process, the parent is presented with the Family Disclosure and "consent[s] to Apple's collection, use, and disclosure of [the] child's information as set forth in Apple's Privacy Policy and this Disclosure." *See* RJN Ex. 18 (Family Disclosure) at 5. The Family Disclosure explains that Apple "may collect things like device identifiers, cookies, IP addresses,

and the geographic locations and time zones in which [the child's] Apple device is used." *Id.* at 4. Apple "may also collect information about [the] child's activities and interactions on our websites, apps, products, and services, including content provided by third-party developers." *Id.* Once a minor turns 13, they are not subject to the Family Disclosure. *See id.* at 3 (a minor who turns 13 can maintain their own account without participating in Family Sharing); RJN Ex. 3 (Privacy Policy) at 6 (defining "child" as "an individual under the age of 13" under U.S. law); 15 U.S.C. § 6501(1) (Children's Online Privacy Protection Act defining child as "an individual under the age of 13").

E. Procedural History and Plaintiffs' Allegations.

In November 2022, "two app developers and security researchers at the software company Mysk" tweeted that certain data was collected by the App Store, Music, TV, Books, and Stocks apps after they turned off the Share [Device] Analytics setting. Compl. ¶ 51. A number of lawsuits soon followed. *See, e.g.*, ECF No. 1. Plaintiffs filed the consolidated complaint on October 6, 2023. ECF No. 115.

Plaintiffs allege that they own iPhones, iPads, or Watches and "regularly use[] mobile applications owned by Apple." Compl. ¶¶ 11-25. Minor plaintiffs A.H. and E.M. do not say which apps they use, *id.* ¶¶ 16, 24, while the other plaintiffs give examples, *see, e.g.*, *id.* ¶¶ 23, 25. Plaintiffs allege that at some unspecified date they turned off Allow Apps to Request to Track and/or Share [Device] Analytics on their devices. *Id.* ¶¶ 11-25 While plaintiffs assert that "Apple accessed and recorded [plaintiffs'] data while [they were] using Apple's mobile applications," *id.*, they do not identify what information Apple purportedly "accessed" about them, from which apps, or what that information supposedly revealed.

Plaintiffs' allegations about data collection through the App Store, Music, TV, Books, and Stocks rest entirely on the Mysk tweets and subsequent press coverage. *Id.* ¶¶ 51-56. While some allege using other apps, they allege no facts at all about those other apps' data collection. Nor could plaintiffs allege in good faith that all apps have the same data practices; their own sources say "the Health and Wallet apps, for example, didn't transmit any analytics data at all, regardless of whether the iPhone Analytics setting was on or off." *See id.* ¶ 56 (citing Gizmodo article available at https://tinyurl.com/2c5a3nh7); *id.* ¶ 53 (citing similar article available at https://tinyurl.com/4xvn6vm7).

Based on these barebones allegations, plaintiffs seek to represent a nationwide class and state subclasses of all "natural persons who had details about hardware and operating system specifications,

performance statistics, and data about how they used their devices and applications tracked and/or collected by Apple while using an Apple app (e.g., App Store, Apple Music, Apple TV, Books, and Stocks) on their mobile Apple device (i.e., iPhone, iPad, or Apple Watch) with the 'Allow Apps to Request to Track' and/or 'Share [Device] Analytics' settings turned off." *Id.* ¶¶ 85-91.[3] Based on this class definition and the lack of any factual allegations about other apps, plaintiffs' claims appear to be based only on App Store, Music, TV, Books, and Stocks.

LEGAL STANDARD

A complaint must "state[] a plausible claim for relief," *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009), meaning the "[f]actual allegations must be enough to raise a right to relief above the speculative level," *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 545 (2007). The Court may consider documents incorporated by reference or subject to judicial notice when deciding a Rule 12(b)(6) motion. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 998 (9th Cir. 2018). Claims that sound in fraud must satisfy Rule 9(b)'s heightened pleading standard. *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009).

ARGUMENT

I. Plaintiffs Have Not Established Standing or Stated a Claim Because They Allege No Facts About Their Own Experiences.

A complaint that does little more than "parrot[] internet musings about things [a defendant] may or may not be doing, and which plaintiffs may or may not have experienced themselves," cannot survive dismissal. *Crittenden v. Apple, Inc.*, 2022 WL 2132224, at *4 (N.D. Cal. June 14, 2022). More than one year has passed since the initial complaint was filed, yet all plaintiffs offer to support their claims are press reports about a few of the apps they mention, speculation about what the alleged collection might reveal, and conclusory allegations that Apple "accessed and recorded" unspecified data when plaintiffs were using "mobile applications owned by Apple." *See, e.g.*, Compl. ¶¶ 11-25, 51-56. Plaintiffs do not allege what data was collected from *them* or any facts about the collection practices of apps beyond those in their

[3] Some plaintiffs allege owning a MacBook or Apple TV, Compl. ¶¶ 12, 14, 18, 19, 20, but do not appear to base claims on those. *Id.* ¶¶ 85-91 (limiting class definition to "mobile Apple device[s]").

class definition. *See id.*[4] They also do not explain why collection of that data violates any law. *Id.* The minor plaintiffs do not even allege which apps they used. *Id.* ¶¶ 16, 24. The bare allegation of unspecified data collection neither establishes Article III standing nor states a claim under Rules 8 or 9(b).

Allegations about plaintiffs' own experiences are particularly important for assessing Article III standing for privacy claims because courts analyze concrete harm under the Supreme Court's *TransUnion* decision "based on the nature of the information at issue." *See Mikulsky v. Noom, Inc.*, 2023 WL 4567096, at *5 (S.D. Cal. July 17, 2023). Where plaintiffs do not allege what information was collected about *them*, courts routinely dismiss claims for lack of concrete harm under Article III. In *Valenzuela v. Keurig Green Mountain, Inc.*, for example, the plaintiff claimed that her privacy was invaded when her conversation with a website's customer service chat feature was recorded. 2023 WL 6609351, at *1 (N.D. Cal. Oct. 10, 2023). The court held that, without "any information at all about the contents of the chat," the plaintiff had alleged only "a bare procedural violation, divorced from any concrete harm." *Id.* at *2. Similarly, in *Lightoller v. Jetblue Airways Corp.*, allegations that third-party software collected "clicks, keystrokes (such as text being entered into an information field or text box), [and] URLs of webpages visited" were insufficient to allege concrete harm. 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023).

The same result follows here. Plaintiffs allege that some apps collect data about clicks or searches, Compl. ¶ 52, but they do not provide any facts about what data was collected from *them* or what that data supposedly revealed. *See also Cook v. GameStop, Inc.*, 2023 WL 5529772, at *4-5 (W.D. Pa. Aug. 28, 2023) (no standing where plaintiff did not allege what her clicks or browsing history revealed about her); *Mikulsky*, 2023 WL 4567096, at *4-5 (same for website chat feature); *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023) (same); *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1188 (N.D. Cal. 2020) (no standing where plaintiffs did not identify any sensitive collected data).

Without factual allegations about what data was collected from them, plaintiffs also cannot state their claims. As this Court and others have held, press reports about what *other people* experienced are

[4] To the extent plaintiffs seek to broaden their claims to other apps, their own sources contradict them and weigh further in support of dismissal. *See id.* ¶¶ 53, 56 (citing Gizmodo articles); *Crittenden*, 2022 WL 2132224, at *3 (citing contradictory evidence in materials plaintiffs invoked as basis for dismissal).

not enough. In *In re Google Assistant Privacy Litigation*, plaintiffs claimed that their confidential conversations were recorded based on (1) a press report and (2) assertions that they "repeatedly" interacted with Google Assistant-enabled devices. 457 F. Supp. 3d 797, 810-11, 817 (N.D. Cal. 2020). The court found these allegations too conclusory to state wiretap, privacy, contract, or UCL claims because they did not show that *plaintiffs* had confidential conversations recorded. *Id.* at 816-17, 827-28, 830, 833, 844. Similarly, where plaintiffs alleged that Google collected location data but did not allege facts about *their* data, this Court dismissed, finding it "entirely speculative that geolocation data was ever collected from a [p]laintiff while at a sensitive or confidential location." *In re Google Location Hist. Litig.*, 428 F. Supp. 3d 185, 199 (N.D. Cal. 2019). Plaintiffs here cannot rely on a press report without any factual allegations about their own experiences. *See Cook*, 2023 WL 5529772, at *6-9 (dismissing WESCA claim); *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1139-42 (E.D. Cal. 2021) (dismissing CIPA claim).

II. Plaintiffs Agreed to the Collection at Issue, Which Defeats All Claims.

The complaint should be dismissed for the additional threshold reason that plaintiffs agreed to any first-party app data collection they experienced. Plaintiffs concede that Apple disclosed the collection, Compl. ¶¶ 103, 134, and use of two unrelated settings does not affect that consent.

"[A] person is not wronged by that to which he or she consents[.]" Black's Law Dictionary (11th ed. 2019) (defining "volenti non fit injuria"); Cal. Civ. Code § 3515 (plaintiff "who consents to an act is not wronged by it"). As a result, courts routinely dismiss claims where, as here, the plaintiffs' conduct manifested consent under applicable law. *See, e.g.*, *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 26 (1994) (plaintiff "must not have manifested by his or her conduct a voluntary consent" to alleged privacy violation); *Silver v. Stripe, Inc.*, 2021 WL 3191752, at *4-5 (N.D. Cal. July 28, 2021) (consent via privacy disclosures defeated CIPA claims); *see also Hicks v. PGA Tour, Inc.*, 897 F.3d 1109, 1120 n.6 (9th Cir. 2018) (affirming dismissal of unjust enrichment claim based on consent); *Hassler v. Sovereign Bank*, 374 F. App'x 341, 344 (3d Cir. 2010) (New Jersey Consumer Fraud Act ("NJCFA") claim failed where account agreement "clearly explained" the challenged actions); *Calhoun v. Google, LLC*, 645 F. Supp. 3d 916, 928 (N.D. Cal. 2022) (consent a defense to contract, implied covenant, and UCL claims).

A. Plaintiffs Agreed to Collection by First-Party Apps.

A plaintiff cannot state a claim where contracts or disclosures notify users of the conduct at issue.

See, e.g., *Silver*, 2021 WL 3191752, at *2-3; *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954 (N.D. Cal. 2017), *aff'd* 745 F. App'x 8 (9th Cir. 2018). This Court's decision in *Smith* is directly on point. There, the defendant's policies "disclose[d] the precise conduct at issue in th[e] case," so plaintiffs' consent barred their CIPA, privacy, and implied covenant claims. *Smith*, 262 F. Supp. 3d at 954-55.

Here, plaintiffs allege that Apple "secretly" collects "details about app usage, app browsing communications, personal information, and information relating to the mobile device itself" through "Apple's proprietary applications." Compl. ¶¶ 1, 4, 50. Like in *Smith*, Apple disclosed this exact collection, barring plaintiffs' claims. Take the App Store as an example. Plaintiffs assert that the App Store collects "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 "device identification numbers, what kind of device was used, the device's screen resolution, the device's keyboard language, and how the user was connected to the internet." Compl. ¶ 52. All of this was disclosed to plaintiffs, and they agreed to the collection by assenting to the software license agreement and using the apps.

To use their devices, plaintiffs were required to agree to the relevant software license. *See* RJN Ex. 1 (iOS/iPadOS 16 Software License) at 1 ("BY USING YOUR DEVICE . . . YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE."); RJN Ex. 2 (watchOS Software License) at 1 (same); Compl. ¶ 103. The software licenses incorporate Apple's Privacy Policy. *See* Compl. ¶ 103.

The Privacy Policy discloses that Apple may collect the types of data plaintiffs complain of here, including "[d]ata about your activity on and use of our offerings, such as app launches within our services, including browsing history; search history; product interaction; crash data, performance and other diagnostic data; and other usage data." *See* RJN Ex. 3 (Privacy Policy) at 3; Compl. ¶¶ 2, 48, 103, 134, 141 (relying on Privacy Policy). The Privacy Policy also discloses that collection may include "[d]ata from which your device could be identified, such as device serial number, or about your device, such as browser type." *See* RJN Ex. 3 (Privacy Policy) at 3.

Apps that provide media services—App Store, TV, Music, iTunes, Books, and Stocks—require more data than "utility apps" like Calculator to support the experiences users expect from these services, including providing purchased content, fighting fraud, and delivering relevant recommendations. *See* RJN Ex. 3 (Privacy Policy) at 3-4. Apps that collect this information provide additional detailed disclosures

tailored to each app. *See id.* at 1 ("[W]e provide data and privacy information embedded in our products and certain features that ask to use your personal data.").

When a user first opens one of these media services apps (e.g., App Store), they are presented with a welcome screen that summarizes the app's data collection and use practices and contains a link to a more detailed disclosure, as depicted in RJN Exhibits 4-8. This welcome screen again discloses the collection plaintiffs challenge here: "Your searches, browsing, purchases, and device trust score may be used to personalize your experience, send you notifications including for Apple marketing, improve the store, and prevent fraud." *See* RJN Ex. 4 (App Store welcome screen). A hyperlink leads to a more detailed disclosure, which is also available online and in the device's Settings. *Id.*; RJN Exs. 5-8.

The App Store & Privacy disclosure explains the app's data collection and use in even greater detail, including, again, the collection plaintiffs challenge here:

Complaint's Allegation	App Store & Privacy Disclosure
App store collects "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." Compl. ¶ 52.	The App Store collects "information about your usage of the stores, including when you open or close the App Store, what content you search for, [and] the content you view and download." RJN Ex. 9 (App Store & Privacy) at 2. "We use your interactions with the App Store to help you discover the content that's most relevant to you. For example, we recommend content that we think will be of interest to you based on what you've previously searched for, viewed, downloaded, updated, or reviewed in the App Store." *Id.* "The information Apple receives about your usage of the stores includes information about the personalized content you tap and view." *Id.*
App Store collects "details about a user's mobile device . . . , including device identification numbers, what kind of device was used, the device's screen resolution, the device's keyboard language, and how the user was connected to the internet." Compl. ¶ 52.	"When you download an app from the App Store, or install an app on your Apple Watch, identifiers such as your device's hardware ID and IP address are logged by Apple along with your Apple ID." RJN Ex. 9 at 1. "We also collect information about your device such as the type of device, the version of your operating system, and the amount of free space on your device. We may use this information to assess whether requested content can be downloaded, to understand general trends in use of device storage, and whether your device is connected by Wi-Fi or cellular." *Id.* at 2.

Complaint's Allegation	App Store & Privacy Disclosure
"Apple collects a 'Directory Services Identifier' that is tied to a mobile device user's iCloud account, and links their name, email address, and more to the harvested user data." Compl. ¶ 55.	"[W]e use information about your browsing, purchases, searches, and downloads. These records may be stored with IP address, a random unique identifier (where that arises), and Apple ID when you are signed in to the App Store or other Apple online stores." RJN Ex. 9 at 1.

The other apps' disclosures are similar. *See* RJN, Exs. 10-13. Plaintiffs proceeded to use these apps after being put on notice of the collection about which they complain. That constitutes consent to the collection under applicable law, and it forecloses all of plaintiffs' claims. *See Silver*, 2021 WL 3191752, at *4 (consent via disclosures defeated privacy claims); *Smith*, 262 F. Supp. 3d at 953-54 (same); *see also Chen v. Dunkin' Brands, Inc.*, 954 F.3d 492, 500 (2d Cir. 2020) (disclosure of challenged practice defeated GBL claim); *Hassler*, 374 F. App'x at 344 (same for NJCFA).

B. Turning Off Unrelated Privacy Controls Does Not Alter Plaintiffs' Consent.

Plaintiffs do not dispute the existence of Apple's service-specific disclosures or argue that they do not encompass the collection they challenge here. *See* Compl. ¶ 103. Instead, plaintiffs contend that a reasonable consumer would believe that turning off the Allow Apps to Request to Track and/or Share [Device] Analytics settings prevents Apple from collecting "mobile device user data." *See id.* ¶ 49. This cannot be reconciled with the explanations of these settings. Plaintiffs' reliance on these unrelated privacy controls is an incurable defect that should result in dismissal with prejudice.

1. The Allow Apps to Request to Track Setting Governs Requests to Track Across Other Companies' Apps and Websites, Which Is Not at Issue Here.

Plaintiffs first invoke the Allow Apps to Request to Track setting: It has nothing to do with Apple's collection and use of data through its own apps, which is all plaintiffs challenge here. The Allow Apps to Request to Track setting governs whether apps can *ask* to track users across apps or websites *owned by other companies*, as Apple's descriptions of the setting consistently make clear. The setting thus does not govern a company's collection and use of data through its own apps without more, and plaintiffs do not and cannot allege that Apple tracked users across *other companies'* apps or websites. *See* Compl. ¶ 1.

Plaintiffs claim the Allow Apps to Request to Track setting "promised that [it] would prevent Plaintiffs' and the Class's user data from being collected while they used an Apple device," *id.* ¶ 104, but that is not what Apple said, as plaintiffs' own allegations repeatedly illustrate. For example, plaintiffs quote the "App Tracking Transparency" support page statement that the setting "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*.'" *Id.* ¶ 44 (emphasis added). That same support page defines "tracking" as occurring "when information that identifies you or your device collected from an app is linked with information that identifies you or your device *collected on apps, websites and other locations owned by third parties*[.]" *See If an app asks to track your activity*, APPLE (Feb. 13, 2023), https://support.apple.com/en-us/HT212025 (emphasis added) (cited in Compl. ¶ 44). Plaintiffs also include a screen shot of the Tracking disclosure, which explains that Apple "requires app developers to ask for permission before they track your activity *across Apps or websites they don't own*." Compl. ¶ 105.

Apple's other descriptions of the Allow Apps to Request to Track setting—including directly below the setting—also contradict plaintiffs' theory. *See Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000) (court need not accept as true allegations contradicted by judicially noticeable facts). The description directly below the setting says, "Allow apps *to ask* to track your activity *across other companies' apps and websites*." *See* RJN Ex. 16 (Allow Apps to Request to Track setting screen) (emphasis added). And the Privacy Policy makes clear that turning off this setting prevents apps from requesting "to track you across apps and websites *owned by other companies*." RJN Ex. 3 (Privacy Policy) at 8 (emphasis added). Plaintiffs do not explain how the Allow Apps to Request to Track setting has any relevance to data collection solely through a company's own apps in light of these uncontested statements.

2. "Share [Device] Analytics" Does Not Control the Data Collection at Issue.

Plaintiffs also misconstrue the Share [Device] Analytics setting. Plaintiffs focus on the Device Analytics & Privacy disclosure's statement that turning off the setting "disable[s] the sharing of Device Analytics altogether.'" *See* Compl. ¶ 46. From this, they implausibly allege that the Share [Device] Analytics setting purports to turn off not only Device Analytics, but all data collection. *See id.* ¶¶ 49, 104, 110. That is not what the disclosure says, and the disclosure's explanation of "Device Analytics" contradicts plaintiffs' theory. In the same disclosure plaintiffs quote, Apple explains that a user can review data included in Device Analytics by clicking "Analytics Data," immediately below the Share [Device] Analytics setting. *See* Compl. ¶¶ 46, 108 (quoting RJN Exs.14, 15); *see id.* ¶ 107 (screen shot showing placement of "Analytics Data"). The disclosure then states that turning off the Share [Device] Analytics setting prevents the sharing of this Device Analytics data. *See* RJN Ex. 14 (Device Analytics & Privacy)

at 1. The Device Analytics & Privacy disclosure does not purport to alter collection of data other than Device Analytics, let alone all "user data . . . collected while [plaintiffs] used an Apple device." Compl. ¶ 104. Plaintiffs offer no explanation for why they would interpret a setting that applies to the defined term "Device Analytics" to also affect collection that enables the services users expect from the apps, including delivery of content.

Because the settings plaintiffs rely on govern data collection unrelated to the alleged collection plaintiffs challenge, the complaint should be dismissed in its entirety with prejudice.

III. The Contract Claims Do Not Identify a Breach or Damages, Among Other Deficiencies.

The breach of contract, implied contract, and implied covenant claims should be dismissed because plaintiffs do not plead breach or damages. The implied contract and unjust enrichment claim cannot proceed because plaintiffs allege that an express contract governs. The implied covenant claim also fails because plaintiffs do not allege that Apple unfairly prevented them from receiving a contracted-for benefit, and the unjust enrichment claim should be dismissed because plaintiffs do not allege any unjust act.

A. Plaintiffs Do Not Allege a Breach of Any Contract.

Plaintiffs cannot establish the required element of breach, which warrants dismissal of the contract, implied contract, and implied covenant claims. *See Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1095 (N.D. Cal. 2022) ("Plaintiffs cannot state a claim for breach of contract without alleging a promise that is breached."); *see also Yari v. Producers Guild of Am., Inc.*, 161 Cal. App. 4th 172, 182 (2008) (implied contract); *Putian Authentic Enter. Mgmt. Co. v. Meta Platforms, Inc.*, 2022 WL 1171034, at *7 (N.D. Cal. Apr. 19, 2022) (implied covenant). Unable to identify any breach of the software licenses or Privacy Policy, plaintiffs contend that the alleged contract "incorporates the mobile device's settings into the terms of the parties' agreement." Compl. ¶ 103. That argument does not save plaintiffs' claims because the settings govern other types of collection not at issue here. *See supra*, Section II.B.

Plaintiffs also are wrong that the Privacy Policy incorporates device settings. The passage they quote says something else: "we provide data and privacy information embedded in our products and certain features . . . You will be given an opportunity to review this product-specific information before using these features. You can view this information at any time, either in Settings related to those features and/or online at apple.com/legal/privacy/data." Compl. ¶ 103. That text incorporates the welcome screens

and service-specific disclosures shown the first time a user opens an app, not the state of a user's settings. Plaintiffs do not identify any promise about the settings, let alone one that was breached. *See Block v. eBay, Inc.*, 747 F.3d 1135, 1138 (9th Cir. 2014) (parties' intent to be ascertained by "the writing alone, . . . the words being interpreted in their ordinary . . . sense, provided that the language is clear").

Nor can the minor plaintiffs pursue contract claims based on Apple's Family Disclosure. *See* Compl. ¶¶ 111-18, 134. *First*, no matter the minor's age, the theory of breach is based on the same settings as the adults' claims and fails for the same reasons. *See id.* ¶¶ 117, 122-24, 136. *Second*, the Family Disclosure and the parental consent procedures it describes apply only to minors under the age of 13. *See* RJN Ex. 3 (Privacy Policy) at 6 (defining child to mean "an individual under the age of 13" in the U.S.); RJN Ex. 18 (Family Disclosure) at 3 (incorporating Privacy Policy and noting U.S. minors aged 13 and up need not use Family Sharing). The minor plaintiffs do not allege their ages, so there is no factual basis to conclude that the Family Disclosure applies. *Third*, if they were under 13 years old, their parents would have set up their accounts and consented consistent with the Family Disclosure, so the complaint could not allege a contract between minor plaintiffs and Apple. *See* RJN Ex. 18 (Family Disclosure) at 3, 5.

B. The Complaint Does Not Plausibly Plead Damages.

Plaintiffs must allege "appreciable and actual damage" resulting from a breach. *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000); *see also Yari*, 161 Cal. App. 4th at 182 (implied contract); *Putian*, 2022 WL 1171034, at *7 (implied covenant). Plaintiffs assert three types of contractual damages, none of which suffices: nominal damages, "the value of their data," and "the premium they paid for Apple mobile devices not to be tracked." Compl. ¶¶ 118, 128, 137.

As this Court has held, "nominal damages and speculative harm, without a showing of actual damages, do[] not suffice." *Rudgayzer v. Yahoo! Inc.*, 2012 WL 5471149, at *6 (N.D. Cal. Nov. 9, 2012); *see Huynh v. Quora, Inc.*, 2019 WL 11502875, at *9 (N.D. Cal. Dec. 19, 2019) (collecting cases).

Plaintiffs' conclusory contention that "the value of their data" decreased fares no better. Compl. ¶¶ 118, 128, 137. While plaintiffs allege that data has value to companies, that does not show any loss to *plaintiffs*. *See, e.g.*, *id.* ¶¶ 60, 63-65; *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *6 (N.D. Cal. June 9, 2023). They claim that other companies' studies paid users to monitor their web-browsing, Compl. ¶¶ 69-71, or that platforms allow users to "own and earn from their data," *id.* ¶ 77, but they do not allege

that they have ever tried to monetize their data, have any plans to, or that the alleged collection of data here prevents them from doing so in the future. Such a "loss in value would not be a cognizable form of contract damages" in any event because contract damages aim to restore plaintiffs to the position they would have been in had the contract been performed. Plaintiffs here do not allege they expected Apple to compensate them for their data, nor could they allege that Apple ever offered to do so. *See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1029 (N.D. Cal. 2012).

Finally, plaintiffs' factual allegations do not support the claim that they paid a premium "for Apple mobile devices not to be tracked." Compl. ¶¶ 118, 128, 137. Out of 15 plaintiffs, seven do not allege ever seeing or relying on any Apple statements whatsoever. *Id.* ¶¶ 11, 14, 16, 17, 21, 22, 24. Six allege reviewing disclosures *after* purchasing their device. *Id.* ¶¶ 12, 15, 19, 20, 23, 25. And six allege being "exposed" to unspecified "advertisements from Apple touting the company's commitment to privacy." *Id.* ¶¶ 12, 13, 15, 18, 20, 25. None alleges relying on any statement about tracking or data collection in deciding to purchase their device. Nor do they allege any facts showing that they paid more than they otherwise would have; the complaint does not contain any allegations about device prices, let alone the amount of any purported premium. *See Schippell v. Johnson & Johnson Consumer Inc.*, 2023 WL 6178485, at *8 (C.D. Cal. Aug. 7, 2023) (collecting cases dismissing conclusory "price premium" claims).

C. The Contract-Related Claims Suffer Other Fatal Flaws.

Plaintiffs' implied contract and unjust enrichment claims also should be dismissed because plaintiffs contend an express contract governs the subject. As this Court has 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); *Nguyen v. Stephens Inst.*, 529 F. Supp. 3d 1047, 1056-57 (N.D. Cal. 2021) (same for unjust enrichment).

Plaintiffs' implied covenant claim is deficient because they identify no benefit of an express contract that Apple unfairly prevented them from receiving, for the reasons explained in Section III.A. *Lee v. Wells Fargo Bank, N.A.*, 2013 WL 1117866 at *5 (N.D. Cal. Mar. 18, 2013). Plaintiffs claim that Apple "reserved discretion to collect consumers' data" by saying in its Privacy Policy that it "may" collect data and abused this discretion by actually collecting it, *see* Compl. ¶¶ 134-35, but courts regularly reject similar arguments. *See Silver*, 2021 WL 3191752, at *4 (collecting cases). Finally, given the extensive

disclosures, plaintiffs have not alleged any unjust conduct by Apple. *See Hicks*, 897 F.3d at 1120 n.6.

IV. The Complaint Does Not Plausibly Allege a Wiretap or Privacy Claim.

A. The Complaint Does Not Allege the Elements of a CIPA Section 632 Claim.

Section 632, enacted in 1967, 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). To address advances in technology, the legislature in 1985 passed Section 632.5 to ensure that CIPA applied to a new technology at that time: cellular phones. *See People v. Guzman*, 8 Cal. 5th 673, 687 (2019). In 1990, it amended CIPA to address another new technology: cordless telephones. *Id.* at 689. Other provisions of CIPA have been amended to account for body-worn cameras, § 633.02(b) (added in 2016); the distribution of confidential health care communications on the internet, § 632.01(a)(1) (2016); satellite television, § 637.5 (1982); and rideshare programs, § 637.6 (1990). Despite multiple changes to account for other technologies, the legislature has not amended CIPA to include data collection. Instead, in 2018, it passed the California Consumer Privacy Act, which comprehensively regulates collection and use of consumers' personal data.

Plaintiffs do not claim that Apple failed to comply with those regulatory requirements. Instead, they attempt to shoehorn a data collection claim into a CIPA provision "designed to combat illicit recording of telephonic communications." *See Quigley v. Yelp, Inc.*, 2018 WL 7204066, at *4 (N.D. Cal. Jan. 22, 2018) (dismissing Section 632 claim based on alleged surveillance of internet communications). The mismatch is fatal: plaintiffs do not satisfy any of the elements of a Section 632 claim, and allowing plaintiffs' claim to proceed would drastically expand CIPA's reach beyond the scope of the statute.

First, plaintiffs do not satisfy the "without consent" element because all parties consented to the collection at issue. *See supra* Section I; *Smith*, 262 F. Supp. 3d at 955.

Second, the conclusory allegation that "Apple's mobile applications constitute an 'amplifying or recording device' under the CIPA" is not sufficient. *See* Compl. ¶ 157. As this Court held in *Google Location History*, a bare legal conclusion that some technology constitutes a device within the meaning of CIPA does not state a claim. 428 F. Supp. 3d at 194 ("The Court need not accept Plaintiffs' bare conclusion that GPS hardware, cellular radios, and WiFi chips qualify as 'electronic tracking devices.'").

Analysis by this Court and another court in this district of an analogous CIPA provision confirms

that the apps here do not qualify as an "amplifying or recording device." In *Google Location History* and *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *5 (N.D. Cal. Dec. 14, 2017), the courts considered whether apps were "location tracking devices" within the meaning of Section 637.7 and concluded they were not. The courts explained that software is not a "device" within the meaning of the statute because it is not "equipment" made for the specific purpose of location tracking. *Google Location Hist.*, 428 F. Supp. 3d at 193-94 (Google Maps app is software, not a "device"); *Moreno*, 2017 WL 6387764, at *5 (same for BART app). The same result follows here. These apps are software designed to provide users with music, information about stocks, or access to other apps. They are not "equipment" primarily designed to "amplify or record." *Cf. Mollaei v. Otonomo Inc.*, 651 F. Supp. 3d 1135, 1140-41 (N.D. Cal. 2023) (following *Google Location History* and *Moreno* to find that an integrated vehicle component was not an "electronic tracking device"); *Mastel*, 549 F. Supp. 3d at 1135 (declining to interpret "telephone device" to include the iOS Pasteboard).

Third, plaintiffs have not adequately alleged that the data collected is a "communication" within the meaning of CIPA. CIPA does not define "communication," but both Black's Law Dictionary and the California Court of Appeal stress the concept of an exchange of ideas. Black's defines communication as "[t]he interchange of messages or ideas by speech, writing, gestures, or conduct; the process of bringing an idea to another's perception." COMMUNICATION, Black's Law Dictionary (11th ed. 2019). The California Court of Appeal has emphasized that CIPA protects against "an intrusion on one's thoughts, ideas, or knowledge." *People v. Drennan*, 84 Cal. App. 4th 1349, 1358 (2000) (still photographs do not violate CIPA because they do not record a "communication"). Because plaintiffs do not specify what actions they took in any app or what data they believe was collected from them, the complaint does not plausibly allege recording of a "communication." Moreover, many of the categories of data that plaintiffs generally allege that Apple might collect plainly are not a "communication" under any definition of the term. For example, plaintiffs allege Apple collects "details about a user's mobile device," "device identification numbers, what kind of device was used, the device's screen resolution, the device's keyboard language, and how the user was connected to the internet." Compl. ¶ 52. Those are facts about a user's device settings, not ideas that a user conveyed to another party. Nor is data about whether a user opened an app or how long a user spends in an app a "communication."

Fourth, plaintiffs do not allege "eavesdrop[ping] upon or record[ing]" within the meaning of CIPA. "California courts interpret 'eavesdrop,' as used in section 632, to refer to a third party secretly listening to a conversation between two other parties." *Google Assistant Priv. Litig.*, 457 F. Supp. 3d at 827. Because the alleged communications are between plaintiffs and Apple apps, Apple is a party to the communications, not a third party, and so the "eavesdrop" clause of Section 632 does not apply. Moreover, collection of data that users provide to Apple is not akin to secretly "recording" a confidential conversation for later playback. Such an expansive interpretation of "recording" would criminalize the everyday occurrence of an intended email recipient saving that email for later reference, which cannot be the law. *See In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *23 (N.D. Cal. Sept. 26, 2013) (dismissing Section 632 claim and observing that "[u]nlike phone conversations, email services are by their very nature recorded on the computer of at least the recipient, who may then easily transmit the communication to anyone else"); *see also TBG Ins. Servs. Corp. v. Super. Ct.*, 96 Cal. App. 4th 443, 452 n.8 (2002) ("any reasonably intelligent person 'savvy enough' to use the Internet is aware that messages are received in a recorded format").

Fifth, plaintiffs fail to allege that their data is a confidential communication within the meaning of Section 632. "Confidential communication" is defined as a communication "in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto," but excludes circumstances where the parties "may reasonably expect that the communication may be . . . recorded." § 632(c). Given Apple's extensive privacy disclosures, no reasonable user would expect that their actions in Apple's apps would be private from Apple. *See Swarts v. Home Depot, Inc.*, 2023 WL 5615453, at *8 (N.D. Cal. Aug. 30, 2023) (allegation that consumers "cannot be expected to know that chat conversations with customer service agents are generally recorded is objectively unreasonable").

Moreover, while phone conversations often are found to be confidential if a party has no reason to believe someone else is listening in, California courts generally presume that written electronic communications "are not 'confidential' within the meaning of [S]ection 632," because they "can easily be shared by, for instance, the recipient(s)." *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014). Plaintiffs do not allege any facts about their app use, so they cannot establish that any communications were "confidential" within the meaning of section 632, let alone overcome the

presumption to the contrary. *See Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1020 (9th Cir. 2013) (allegation that plaintiff called to dispute a charge not enough detail about the context to establish an objectively reasonable expectation of confidentiality); *Rodriguez v. Google LLC*, 2021 WL 2026726, at *7 (N.D. Cal. May 21, 2021) (sensitivity of users' online queries and browsing histories did not make data "confidential" under Section 632); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) ("browsing activity and form field entries" on a website not confidential communications).

The complaint's failure to adequately plead multiple elements of the CIPA claim underscores the gulf between CIPA's statutory language and plaintiffs' attempted use of it here. Allowing plaintiffs to proceed based on ordinary collection of data about the screen resolution or keyboard language of a device would expand CIPA far beyond its intent of prohibiting eavesdropping on conversations. *See Drennan*, 84 Cal. App. 4th at 1355-58; *Quigley*, 2018 WL 7204066, at *4. The legislature knows how to amend CIPA to account for new technologies and has done so repeatedly in the past, but it has not done so for the app data collection at issue here. *See Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 202 n.10 (2021). Expansively interpreting a criminal statute like CIPA in a way that departs from the legislative goal would violate not only the rules of statutory interpretation but also the rule of lenity. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009) (rule of lenity applies to civil claim under penal statute).

B. The Complaint Does Not Allege the Elements of a WESCA Claim.

WESCA is Pennsylvania's statute that "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). As relevant here, it prohibits the intentional interception of the contents of any electronic communication. 18 Pa. C.S. § 5703. Plaintiffs fail to allege any of the elements of an unlawful interception claim under WESCA.

First, plaintiffs consented to the alleged data collection at issue, and the statute permits collection with the parties' "prior consent." *Id.* § 5704(4); *see also supra* Section II; *Popa*, 52 F.4th at 126, 133.

Second, plaintiffs do not allege an "interception" under WESCA because Apple did not obtain the "contents" of any "communication." WESCA defines "contents" as "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).

Under the federal statute, courts have recognized that the term "contents" does not include "record information," *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014), such as "addresses, phone numbers, and URLs" when performing a "dialing, routing, addressing or signaling function," *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 137 (3d Cir. 2015).

Plaintiffs have not alleged the collection of "content" within the meaning of WESCA. They assert that Apple collects "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." Compl. ¶¶ 52, 186. This information does not constitute "the substance, purport, or meaning"—*i.e.*, the "contents"—of communications under WESCA; rather, it is "record information" describing how a user interacts with the apps. *See Zynga*, 750 F.3d at 1106; *see also S.D. v. Hytto Ltd.*, 2019 WL 8333519, at *6 (N.D. Cal. May 15, 2019) (under the Federal Wiretap Act, "the origin of a phone call, a phone call's length, and geolocation data from an app," as well as the "date and time of usage data" collected are not "content," but "record information"); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082-83 (C.D. Cal. 2021) (clicks, pages visited, keystrokes, and PII, including shipping and billing information, are not "contents" under California's analogous wiretap statute).

Third, plaintiffs fail to plausibly allege collection by a "device," as required to state a claim. *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, at *4 (E.D. Pa. Dec. 13, 2007). WESCA defines a "device" as "[a]ny device or apparatus . . . that can be used to intercept a wire, electronic or oral communication." 18 Pa. C.S. § 5702. However, the device performing the alleged interception must be separate from the source of the communication. *See Commonwealth v. Diego*, 119 A.3d 370, 374 (Pa. Super. 2015) (finding that an iPad from which the intercepted communication originated was not the relevant device). Here, plaintiffs allege that their mobile devices are the intercepting devices under WESCA, Compl. ¶ 185, and also the sources of the purportedly intercepted communications. *Id.* ¶¶ 1, 11-25 (stating that Apple collects "users' data when they interact with Apple's proprietary applications . . . on their mobile Apple devices"). That is fatal to their WESCA claims. *See Diego*, 119 A.3d at 374.

Fourth, the WESCA claim fails because Apple was the direct recipient of any communications. The Pennsylvania Supreme Court has held that where, as here, "a party receives information from a communication as a result of being a direct party to the communication, there is no interception." *See*

Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. 2001), *aff'd*, 837 A.2d 1163 (Pa. 2003).

Plaintiffs' citation to the Third Circuit's decision in *Popa*, 52 F.4th at 124, does not change the result. That decision is not binding on this court, *see Rivera v. Invitation Homes, Inc.*, 2019 WL 11863726, at *2 (N.D. Cal. June 19, 2019), and diverges from the Pennsylvania state court decisions that have consistently recognized the direct-party exception. *See Commonwealth v. Cruttenden*, 58 A.3d 95, 98-100 (Pa. 2012); *Proetto*, 771 A.2d at 831; *Diego*, 119 A.3d at 380-81. Moreover, *Popa* does not apply on its facts. There, the court stated that the plaintiff "obviously knew" her browser was communicating with the website she was viewing (operated by defendant) but did not know that her browser was *also* communicating with a third-party marketing company. *Popa*, 52 F.4th at 124. Here, plaintiffs "obviously knew" they were interacting with Apple when using Apple's apps and do not allege that any data was transmitted to any third party. Under these facts, *Popa* does not apply.

C. Apple Did Not Invade Plaintiffs' Privacy.

Apple believes that privacy is a fundamental human right and designs its products and services with privacy in mind. The allegations plaintiffs advance here do not support their claims for violations of the California constitutional privacy right. "The California Constitution sets a 'high bar' for establishing an invasion of privacy claim." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014). 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." *Hill*, 7 Cal. 4th at 35-37. The complaint's sparse allegations do not satisfy these elements.

1. No Legally Protected Privacy Interest Is at Issue on These Sparse Facts.

California law recognizes two classes of legally protected privacy interests: (1) informational privacy, which is the interest in "precluding the dissemination or misuse of sensitive and confidential information," and (2) autonomy privacy, which is the interest in "making intimate personal decisions or conducting personal activities without observation, intrusion, or interference." *Google Location Hist.*, 428 F. Supp. 3d at 196-97. The complaint's limited facts do not satisfy either.

An informational privacy interest is not adequately pleaded because plaintiffs do not allege any facts about how, if at all, they used the Apple apps or the information about them Apple allegedly collected through these apps. *See* Compl. ¶¶ 11-25; *supra* Section I. Plaintiffs' bare allegations that their data was

collected do not establish that the alleged collection involved "sensitive and confidential information," let alone that the information was disseminated or misused. *See Google Location Hist.*, 428 F. Supp. 3d at 196-99. That is particularly true where, as here, a reasonable consumer would understand that an app provider collects certain data from the app to provide and improve the requested services. *See Yoon*, 549 F. Supp. 3d at 1086 (no informational privacy interest in user activity on company's own website).

Nor is autonomy privacy at issue on the sparse allegations here. As this Court recognized in *Google Location History*, "California courts have discussed autonomy privacy in cases 'alleging *bodily* autonomy.'" 428 F. Supp. 3d at 198. Plaintiffs do not identify anything about the information purportedly collected about them, let alone something that would implicate their bodily autonomy or provide grounds for extending the right more broadly. *See id.*; *see also Yoon*, 549 F. Supp. 3d at 1086 (agreeing with *Google Location History*'s refusal to extend autonomy privacy beyond bodily autonomy).

2. Plaintiffs Do Not Plead a Reasonable Expectation of Privacy in Data They Knowingly Agreed to Disclose.

Plaintiffs fail to plead the second element for two reasons. *First*, as discussed above, Apple disclosed the collection, and plaintiffs agreed to it through the software license agreement, when first using each app, and by continuing use of each app. "[T]he plaintiff in an invasion of privacy case must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant." *Hill*, 7 Cal. 4th at 26. Because plaintiffs used the apps after Apple's extensive disclosure of data collection, they cannot now claim that they had a reasonable belief that same collection would not occur. *See Smith*, 262 F. Supp. 3d at 955-56 (collecting cases holding that consent bars a privacy claim).

Second, plaintiffs cannot reasonably expect that data they knowingly provide to Apple would not be received by Apple. In *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), for example, the Ninth Circuit held that internet users do not have a reasonable expectation of privacy in the to/from addresses of e-mail messages or the IP addresses of websites visited "because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *Id.* at 510; *see also Heeger*, 509 F. Supp. 3d at 1189-90 (same). The same is true here. Reasonable consumers understand, for example, that when they buy a book in the Books app, Apple must record the purchase to process the transaction and make the book available on users' devices. *Cf. Gmail*

Litig., 2013 WL 5423918, at *23 (expectation of privacy in emails inadequately alleged because emails "are by their very nature recorded on the computer of at least the recipient").

The fact that plaintiffs challenge only the collection and use of data within the first-party Apple apps—where Apple receives certain information to provide services—also distinguishes this case from those involving alleged third-party collection of user data from apps or websites owned by other companies. *See, e.g.*, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 603 (9th Cir. 2020) (alleged collection included data from other websites using Facebook plug-in); *Rodriguez*, 2021 WL 2026726, at *3, 8 (alleged collection from third-party apps using Google Firebase analytics). As in *Forrester* and in contrast to *Facebook Internet Tracking* and *Rodriguez*, Plaintiffs do not adequately allege that they reasonably believed Apple's data collection within its own apps—which allows Apple to operate those apps as users expect—would not occur.

3. Disclosed Data Collection Is Not an "Egregious Breach" of Social Norms.

The privacy claim also fails to state the third element: that the alleged collection is "so serious 'in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.'" *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009). Courts regularly dismiss claims under this element where the plaintiffs do not plead facts showing that the data collected from them was sensitive. For example, in *Mastel*, the plaintiff alleged that an app secretly accessed the iPhone's Pasteboard, which allows users to copy text between apps. 549 F. Supp. 3d at 1132-33. The Pasteboard allegedly may have contained "his contact information, addresses for his friends and relatives, or text from messages that he had sent." The court found that accessing such information was not an egregious breach without any allegation the information was sensitive. *See id.* at 1141-42; *see also Heeger v. Facebook, Inc.*, 2019 WL 7282477, at *4 (N.D. Cal. Dec. 27, 2019) (conclusory allegation that defendant accessed "private" location data insufficient). Here, the complaint's sole allegation about plaintiffs' app use is that they "regularly use[] mobile applications owned by Apple." Compl. ¶¶ 11-25. The complaint says nothing about what information Apple allegedly gathered about plaintiffs, let alone why any such information was sensitive.

Setting aside the fatal defect of plaintiffs' failure to allege what if any data was collected from them, plaintiffs' general hypotheses about what categories of information might have been collected also do not state a claim. "Many courts have found that the collection—and even disclosure to certain third

parties—of personal information about the users of a technology may not constitute a sufficiently egregious breach of social norms to make out a . . . constitutional privacy claim." *McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *7 (N.D. Cal. Feb. 2, 2021). Instead, "courts have characterized the collection and disclosure of such data as 'routine commercial behavior,'" which is insufficient to state a claim. *Id.*

In *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012), for example, the plaintiffs alleged that third-party apps collected "Plaintiffs' addresses and current whereabouts; the unique device identifier ('UDID') assigned to the iDevice; the user's gender, age, zip code and time zone; and app-specific information such as which functions Plaintiff performed on the app." *Id.* at 1050. The court concluded that, "[e]ven assuming this information was transmitted without Plaintiffs' knowledge and consent, . . . such disclosure does not constitute an egregious breach of social norms." *Id.* at 1063; *see also Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) (collecting customer data during in-store transactions and disclosing to third party for marketing without customer's awareness did not state claim); *In re Google, Inc. Privacy Pol'y Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (disseminating data from Google services did not allege serious invasion under analogous tort of intrusion upon seclusion); *Low*, 900 F. Supp. 2d at 1025 (disclosing LinkedIn browsing history not an egregious breach).

More recently, two courts in this district found that collecting data on the frequency and duration of app use was not an egregious breach. In *McCoy v. Alphabet Inc.*, the court held that Google's alleged monitoring of "confidential and sensitive data," including "when and how often . . . non-Google apps are used and the amount of time a user spends on . . . non-Google apps" did "not rise to the requisite level of an egregious breach of social norms." 2021 WL 405816, at *1, *8. In *Hammerling v. Google LLC*, the plaintiff alleged that Google could have discerned plaintiffs' bank, type of car, and interest in religion, among other things. 2022 WL 17365255, at *1 (N.D. Cal. Dec. 1, 2022). But the court held that "Hammerling's searches of a foot massager, slippers, meal subscriptions, coconut oil, and use of a photo editor are better characterized as data collection of "'routine commercial behavior,' not considered a highly offensive intrusion of privacy in this district." *Id.* at *8-9. Plaintiffs here provide even less detail than in *Hammerling*, so have not alleged an egregious breach as a matter of law.

V. The State-Law Consumer-Protection Claims Fail for Several Reasons.

Plaintiffs assert violations of California, New York, New Jersey, and Illinois consumer protection

laws. These claims invoke different statutes, but they all require a fraudulent statement or deceptive act. *See* Cal. Bus. & Prof. Code § 17200; N.Y. Gen. Bus. Law §§ 349, 350; N.J. Stat. Ann. § 56:8-1; 815 Ill. Comp. Stat. Ann. 505/1. They also are all premised on the assertions that either (1) Apple promised that the two settings would prevent all types of data collection, or (2) Apple failed to warn that certain data would be collected despite those settings. *See* Compl. ¶¶ 4, 104, 165(e). Because those theories sound in fraud, they must satisfy Rule 9(b)'s heightened pleading requirement, which plaintiffs' claims do not meet.

A. The Misrepresentation Theory Is Not Adequately Alleged.

For claims based on alleged misrepresentations, Rule 9(b) requires plaintiffs to identify, at a minimum, the content of the alleged misrepresentations, "when [they] w[ere] exposed to them," and which they relied upon, *Kearns*, 567 F.3d at 1126, "as well as what is false or misleading about [any] purportedly fraudulent statement, and why it is false," *Salameh v. Tarsadia Hotel*, 726 F.3d 1124, 1133 (9th Cir. 2013).

Plaintiffs' core theory in each of the consumer-protection claims is that the Allow Apps to Request to Track and Share [Device] Analytics settings "promised that they would prevent Plaintiffs' and the Class's user data from being collected while they used an Apple device." Compl. ¶ 104; *see also id.* ¶¶ 1, 5, 49, 50, 165, 246, 265. But the complaint does not identify *any* statement by Apple actually saying that. Instead, the Privacy Policy and service-specific disclosures expressly disclose the complained-of collection. Moreover, the settings and related disclosures specify that they govern (1) requests to track across third-party apps/websites, and (2) certain device performance data, neither of which is at issue here.

Plaintiffs identify other statements, including (1) interviews, articles, billboards, and advertisements regarding Apple's commitment to privacy as a general principle, *see id.* ¶¶ 32-34, 36-43; (2) the Privacy Policy and app-specific disclosures, *see id.* ¶¶ 46-47, 49, 105-07; and (3) an Apple support page explaining the Allow Apps to Request to Track setting, *see id.* ¶¶ 44-45. These allegations do not satisfy Rule 9(b) and do not otherwise identify actionable misrepresentations for multiple reasons.

No reliance. Rule 9(b) requires plaintiffs to specify when they were exposed to the purported misleading statements and whether they relied on them. *Kearns*, 567 F.3d at 1126. Here, seven plaintiffs do not allege ever seeing or relying on any statement by Apple. *See* Compl. ¶¶ 11, 14, 16, 17, 21, 22, 24. While the other six plaintiffs allege generally relying on privacy-related advertising, *id.* ¶¶ 12, 13, 15, 18, 20, 25, they do not specify *which* advertisements they viewed or when, as Rule 9(b) requires. *Kearns*,

567 F.3d at 1126. Six plaintiffs allege reviewing written disclosures that came with their devices *after* purchase, Compl. ¶¶ 12, 15, 19, 20, 23, 25, so they could not have relied on these when making their purchase. *See Hammerling*, 2022 WL 17365355, at *6 (no reliance where plaintiff did not allege reading privacy policy before purchase). These deficiencies alone require dismissal. *See Tabak v. Apple, Inc.*, 2020 WL 9066153, at *9 (N.D. Cal. Jan. 30, 2020) (actual reliance required for statutory standing under UCL); *Morrissey v Nextel Partners, Inc.*, 72 A.D.3d 209, 217 (N.Y. 2010) (similar for GBL § 350); *Oliveira v. Amoco Oil Co.*, 776 N.E.2d 151, 155 (Ill. 2002) (advertisements did not "proximately cause" plaintiff's injury under ICFA without allegation plaintiff "saw, heard, or read" them); *Mladenov v. Wegmans Food Markets, Inc.*, 124 F. Supp. 3d 360, 377 (D.N.J. 2015) (NJCFA claim lacked "causal nexus" between the misrepresentation and loss where plaintiffs did not allege which ads they viewed or the "specific times, dates, or places" of the ads).

No false or misleading statements. Plaintiffs identify several statements regarding the Allow Apps to Request to Track or Share [Device] Analytics settings, but as demonstrated above, Apple's descriptions of those settings are not misleading; to the contrary, they make clear these settings do not affect the collection plaintiffs challenge here. *See* Compl. ¶¶ 44-46, 105; *supra* Section II.B. Moreover, Apple's statements in its policies and disclosures cannot support a GBL Section 350 claim because they are not advertising. *See Cohen v. Casper Sleep Inc.*, 2018 WL 3392877, at *9 (S.D.N.Y. July 12, 2018).

Non-measurable statements of product superiority. The other statements plaintiffs identify, such as "Privacy. That's iPhone," are non-measurable statements that are not actionable in fraud. *See Castaneda v. Amazon.com, Inc.*, 2023 WL 4181275, at *7 (N.D. Ill. June 26, 2023) (ads touting "lightning fast loading" of PlayStation 5 not actionable under ICFA); *Lugones v. Pete and Gerry's Organic, LLC*, 440 F. Supp. 3d 226, 241 (S.D.N.Y. 2020) ("better lives for hens mean better eggs for you" not actionable under GBL §§ 349, 350); *Elias v. Hewlett-Packard Co.*, 903 F. Supp. 2d 843, 855 (N.D. Cal. 2012) (ads that computer is "ultra-reliable" and "packed with power" not actionable under UCL); *Rodio v. Smith*, 123 N.J. 345, 352 (1991) ("You're in good hands with Allstate" not actionable under NJCFA).

B. The Omission Theory Does Not Satisfy Rule 9(b).

Plaintiffs also assert that Apple failed to disclose that data would still be collected even after turning off the Allow Apps to Request to Track and Share [Device] Analytics settings. *See* Compl. ¶ 4.

This omission theory fails for three reasons: (1) Apple already discloses the information, (2) it does not satisfy Rule 9(b), and (3) plaintiffs do not adequately allege a duty to disclose.

First, plaintiffs' omission theory cannot survive because the Privacy Policy, welcome screens, and service-specific disclosures *do* disclose the complained-of data collection. *See, e.g.*, *Kumandan v. Google LLC*, 2022 WL 103551, at *8-9 (N.D. Cal. Jan. 11, 2022).

Second, Rule 9(b) requires plaintiffs to allege with particularity that, had Apple made specific disclosures, plaintiffs would have been aware of them and would not have purchased their devices. *See Tabak*, 2020 WL 9066153, at *9; *cf. Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1225 (9th Cir. 2015) (plaintiffs must show "that, had the omitted information been disclosed, one would have been aware of it and behaved differently"). In *Tabak*, for example, plaintiffs alleged they "would not have purchased the devices at issue if they had known about the defect." 2020 WL 9066153, at *9. The court found these allegations "lack[ed] specific factual matter to raise the reasonable inference that, had Apple disclosed information about the defect, Plaintiffs 'would have been aware of it and behaved differently.'" *Id.* Here, plaintiffs assert, without factual support, that they "would not have purchased their devices from [Apple] or would have paid less for them" had they known about the alleged data collection. *See* Compl. ¶¶ 171, 209, 232, 249, 269. These allegations are indistinguishable from those in *Tabak*.

Third, the complaint does not identify a legal basis for any duty to disclose. *See, e.g.*, *Eidmann v. Walgreen Co.*, 522 F. Supp. 3d 634, 646-47 (N.D. Cal. 2021) (UCL); *Gold v. Lumber Liquidators, Inc.*, 2015 WL 7888906, at *11 (N.D. Cal. Nov. 30, 2015) (GBL, ICFA); *Arcand v. Brother Int'l. Corp.*, 673 F. Supp. 2d 282, 297 (D.N.J. 2009) (NJCFA). A duty to disclose exists only when a defendant (1) is the plaintiff's fiduciary, (2) has exclusive knowledge of material facts not known to the plaintiff, (3) actively conceals a material fact from the plaintiff, or (4) makes misleading partial representations. *Eidmann*, 522 F. Supp. 3d at 646. Plaintiffs have not alleged facts going to any of these scenarios. *See Tietsworth v. Sears, Roebuck & Co.*, 2009 WL 3320486, at *4, *8 (N.D. Cal. Oct. 13, 2009) (no duty based on "conclusory" allegations of "exclusive knowledge" and "active concealment").

C. Plaintiffs Do Not Allege Cognizable Damages.

Plaintiffs must allege the loss of money or property to establish statutory standing or plead a claim under the consumer protection laws. *See Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 739-40

(7th Cir. 2014) (ICFA requires "actual damages"); *Small v. Lorillard Tobacco Co.*, 94 N.Y.2d 43, 56 (1999) (GBL requires "either pecuniary or 'actual' harm"); *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 323 (2011) (UCL requires "lost money or property"); *Solo v. Bed Bath & Beyond, Inc.*, 2007 WL 1237825, at *3 (D.N.J. Apr. 26, 2007) (NJCFA requires "ascertainable loss of moneys or property").

Plaintiffs allege that Apple "deprived Plaintiffs and Class Members of the economic value of their user data." Compl. ¶ 84. That theory fails for the reasons explained in Section III.B. And an invasion of privacy, even if that had occurred here, is insufficient to establish "compensable damages" for the relevant claims. *See Williams v. What If Holdings, LLC*, 2022 WL 17869275, at *4 (N.D. Cal. Dec. 22, 2022) (alleged unauthorized recording of data does not establish injury under UCL); *see also Kurowski v. Rush Sys. for Health*, 2023 WL 4707184, at *6 (N.D. Ill. July 24, 2023) (invasion of privacy not "actual damages" under ICFA); *White v. Samsung Elecs. Am., Inc.*, 2019 WL 8886485, at *3-4 (D.N.J. Aug. 21, 2019) (acquisition of personal data without consent not an ascertainable loss under NJCFA); *Cohen*, 2018 WL 3392877, at *7-9 (alleged privacy invasion not a cognizable injury under GBL).

Plaintiffs also allege without elaboration that they would not have used the Apple apps or purchased their devices, or would have paid less for their devices. *See* Compl. ¶¶ 171, 208-09, 231-32, 248-49, 268-69. Conclusory allegations of overpayment do not allege cognizable damages under the consumer protection laws. *See Naimi v. Starbucks Corp.*, 798 F. App'x 67, 70 (9th Cir. Dec. 20, 2019) (GBL); *Camasta*, 761 F.3d at 739-40 (ICFA); *Gerritsen v. FCA US LLC*, 2020 WL 3841304, at *1 (C.D. Cal. Mar. 3, 2020) (UCL); *White*, 2019 WL 8886485, at *3 (NJCFA). The price premium theory also fails because plaintiffs cannot have paid a premium for features they do not allege being aware of before purchase. *See supra*, Section III.B. Moreover, Allow Apps to Request to Track was introduced in 2021, *after* many plaintiffs bought their devices. Finally, the damages allegations also are deficient for the GBL claim to the extent they (1) seek to recover the entire purchase price, or (2) duplicate the contract damages plaintiffs seek. *See Orlander v. Staples, Inc.*, 802 F.3d 298, 302 (2d Cir. 2015); *Small*, 94 N.Y. 2d at 56.

D. None of the California UCL Prongs Are Satisfied.

Because plaintiffs have not alleged a misrepresentation or omission with the particularity required by Rule 9(b), they also cannot satisfy the UCL's "fraudulent" or "unlawful" prongs. *See In re Apple Processor Litig.*, 2022 WL 2064975, at *12 (N.D. Cal. June 8, 2022) (dismissing such claims that were

predicated on same allegations as other failed claims). While plaintiffs refer to COPPA in passing, Compl. ¶ 165(f)), merely listing laws, without alleging facts showing how a defendant violated them, does not state an "unlawful" claim. *See Doe v. CVS Pharmacy, Inc.*, 982 F.3d 1204, 1214 (9th Cir. 2020).

Finally, the "unfair" prong does not support plaintiffs' claim because they do not identify a specific constitutional, statutory, or regulatory provision to which their claim is tethered. *See Drum v. San Fernando Valley Bar Ass'n*, 182 Cal. App. 4th 247, 257 (2010). Nor have plaintiffs alleged facts plausibly showing that Apple's purported conduct is "unethical, oppressive, unscrupulous, or substantially injurious." *Id.* Plaintiffs also claim, without offering any factual basis, that Apple's alleged conduct is "not outweighed by any countervailing benefits to consumer or competition," Compl. ¶ 166, but such a "conclusory recitation" of the balancing test is insufficient. *See Doe*, 982 F.3d at 1214-15.

VI. The Court Lacks Equitable Jurisdiction to Hear the UCL and Unjust Enrichment Claims.

The existence of an adequate legal remedy deprives a court of equitable jurisdiction. *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020). Plaintiffs thus "must plead inadequate legal remedies" to pursue UCL or unjust enrichment claims. *See, e.g.*, *Riordan v. W. Digital Corp.*, 2023 WL 6462857, at *9 (N.D. Cal. Sept. 29, 2023) (dismissing UCL claim under *Sonner*); *Apple Processor Litig.*, 2022 WL 2064975, at *11-12 (same for unjust enrichment). Here, the complaint seeks the legal remedy of damages under CIPA, WESCA, and GBL. Compl. ¶¶ 148, 159, 192, 216, 239. The Court thus lacks equitable jurisdiction. Plaintiffs attempt to avoid dismissal of the equitable claims by contending that (1) legal remedies are not as certain and prompt as equitable relief, and (2) the Court may award restitution even if plaintiffs do not prove their legal claims. *See id.* ¶ 287. Those assertions misunderstand the inquiry—the question is not whether the elements of the legal and equitable claims differ, but rather whether the legal claims adequately can remedy any alleged harm. Since plaintiffs identify no reason the legal claims are inadequate, the UCL and unjust enrichment claims cannot proceed.

CONCLUSION

For the reasons stated, the complaint should be dismissed with prejudice.

Dated: December 8, 2023

Respectfully submitted,

/s/ Kathryn E. Cahoy

Emily Johnson Henn (Bar No. 269482)
Kathryn E. Cahoy (Bar No. 298777)
COVINGTON & BURLING LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306-2112
Telephone: (650) 632-4700
Facsimile: (650) 632-4800
Email: ehenn@cov.com
Email: kcahoy@cov.com

Amy S. Heath (Bar No. 312516)
COVINGTON & BURLING LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
Telephone: (415) 591-7030
Facsimile: (415) 955-6530
Email: aheath@cov.com

Attorneys for Defendant Apple Inc.