

1 Emily Johnson Henn (Bar No. 269482)
2 Kathryn E. Cahoy (Bar No. 298777)
3 COVINGTON & BURLING LLP
4 3000 El Camino Real
5 5 Palo Alto Square, 10th Floor
6 Palo Alto, CA 94306-2112
7 Telephone: (650) 632-4700
8 Facsimile: (650) 632-4800
9 Email: ehenn@cov.com
10 Email: kcahoy@cov.com

11 Amy S. Heath (Bar No. 312516)
12 COVINGTON & BURLING LLP
13 Salesforce Tower
14 415 Mission Street, Suite 5400
15 San Francisco, CA 94105-2533
16 Telephone: (415) 591-7030
17 Facsimile: (415) 955-6530
18 Email: aheath@cov.com

19 *Attorneys for Defendant Apple Inc.*

20 **UNITED STATES DISTRICT COURT**
21 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
22 **SAN JOSE DIVISION**

23 IN RE APPLE DATA PRIVACY LITIGATION

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

24 **DEFENDANT’S NOTICE OF MOTION**
25 **AND MOTION TO DISMISS**
26 **CONSOLIDATED COMPLAINT;**
27 **MEMORANDUM OF POINTS AND**
28 **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

1

2 NOTICE OF MOTION AND MOTION..... 1

3 MEMORANDUM IN SUPPORT: INTRODUCTION AND STATEMENT OF ISSUES..... 1

4 STATEMENT OF FACTS..... 2

5 A. Apple Privacy Disclosures and App Data Collection. 2

6 B. Device Analytics Data and the Share [Device] Analytics Setting. 4

7 C. The Allow Apps to Request to Track Setting..... 5

8 D. Parental Consent for Children Under the Age of 13. 5

9 E. Procedural History and Plaintiffs’ Allegations. 6

10 LEGAL STANDARD 7

11 ARGUMENT 7

12 I. PLAINTIFFS HAVE NOT ESTABLISHED STANDING OR STATED A CLAIM

13 BECAUSE THEY ALLEGE NO FACTS ABOUT THEIR OWN EXPERIENCES..... 7

14 II. PLAINTIFFS AGREED TO THE COLLECTION AT ISSUE, WHICH DEFEATS ALL

15 CLAIMS..... 9

16 A. Plaintiffs Agreed to Collection by First-Party Apps. 9

17 B. Turning Off Unrelated Privacy Controls Does Not Alter Plaintiffs’ Consent. 12

18 III. THE CONTRACT CLAIMS DO NOT IDENTIFY A BREACH OR DAMAGES,

19 AMONG OTHER DEFICIENCIES..... 14

20 A. Plaintiffs Do Not Allege a Breach of Any Contract..... 14

21 B. The Complaint Does Not Plausibly Plead Damages. 15

22 C. The Contract-Related Claims Suffer Other Fatal Flaws. 16

23 IV. THE COMPLAINT DOES NOT PLAUSIBLY ALLEGE A WIRETAP OR PRIVACY

24 CLAIM. 17

25 A. The Complaint Does Not Allege the Elements of a CIPA Section 632 Claim. 17

26 B. The Complaint Does Not Allege the Elements of a WESCA Claim. 20

27 C. Apple Did Not Invade Plaintiffs’ Privacy. 22

28 V. THE STATE-LAW CONSUMER-PROTECTION CLAIMS FAIL FOR SEVERAL

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

REASONS..... 25

A. The Misrepresentation Theory Is Not Adequately Alleged. 26

B. The Omission Theory Does Not Satisfy Rule 9(b). 27

C. Plaintiffs Do Not Allege Cognizable Damages..... 28

D. None of the California UCL Prongs Are Satisfied..... 29

VI. THE COURT LACKS EQUITABLE JURISDICTION TO HEAR THE UCL AND
UNJUST ENRICHMENT CLAIMS..... 30

CONCLUSION 30

TABLE OF AUTHORITIES

Cases

Aguilera v. Pirelli Armstrong Tire Corp.,
223 F.3d 1010 (9th Cir. 2000)..... 15

In re Apple Processor Litig.,
2022 WL 2064975 (N.D. Cal. June 8, 2022) 29, 30

Arcand v. Brother Int’l. Corp.,
673 F. Supp. 2d 282 (D.N.J. 2009)..... 12, 27, 28, 29

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 7

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 7

Block v. eBay, Inc.,
747 F.3d 1135 (9th Cir. 2014)..... 15

Byars v. Sterling Jewelers, Inc.,
2023 WL 2996686 (C.D. Cal. Apr. 5, 2023)..... 8

Calhoun v. Google, LLC,
645 F. Supp. 3d 916 (N.D. Cal. 2022)..... 9

Camasta v. Jos. A. Bank Clothiers, Inc.,
761 F.3d 732 (7th Cir. 2014)..... 28, 29

Campbell v. Facebook Inc.,
77 F. Supp. 3d 836 (N.D. Cal. 2014)..... 19

Castaneda v. Amazon.com, Inc.,
2023 WL 4181275 (N.D. Ill. June 26, 2023) 27

Chen v. Dunkin’ Brands, Inc.,
954 F.3d 492 (2d Cir. 2020) 12

Cohen v. Casper Sleep Inc.,
2018 WL 3392877 (S.D.N.Y. July 12, 2018)..... 27, 29

Commonwealth v. Cruttenden,
58 A.3d 95 (Pa. 2012) 22

Commonwealth v. Diego,
119 A.3d 370 (Pa. Super. 2015) 21, 22

1 *Commonwealth v. Proetto*,
 771 A.2d 823 (Pa. Super. 2001) 22

2

3 *Cook v. GameStop, Inc.*,
 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023)..... 8, 9

4 *Crittenden v. Apple, Inc.*,
 2022 WL 2132224 (N.D. Cal. June 14, 2022) 7, 8

5

6 *Daniel v. Ford Motor Co.*,
 806 F.3d 1217 (9th Cir. 2015)..... 28

7

8 *Doe v. CVS Pharmacy, Inc.*,
 982 F.3d 1204 (9th Cir. 2020)..... 30

9 *Drum v. San Fernando Valley Bar Ass’n*,
 182 Cal. App. 4th 247 (2010)..... 30

10

11 *Eidmann v. Walgreen Co.*,
 522 F. Supp. 3d 634 (N.D. Cal. 2021)..... 28

12

13 *Elias v. Hewlett-Packard Co.*,
 903 F. Supp. 2d 843 (N.D. Cal. 2012)..... 27

14 *In re Facebook, Inc. Internet Tracking Litig.*,
 956 F.3d 589 (9th Cir. 2020)..... 24

15

16 *Faulkner v. ADT Sec. Servs., Inc.*,
 706 F.3d 1017 (9th Cir. 2013)..... 20

17

18 *Folgelstrom v. Lamps Plus, Inc.*,
 195 Cal. App. 4th 986 (2011)..... 25

19 *Fraser v. Nationwide Mut. Ins. Co.*,
 352 F.3d 107 (3d Cir. 2003)..... 20

20

21 *Gerritsen v. FCA US LLC*,
 2020 WL 3841304 (C.D. Cal. Mar. 3, 2020) 29

22

23 *Gold v. Lumber Liquidators, Inc.*,
 2015 WL 7888906 (N.D. Cal. Nov. 30, 2015)..... 28

24 *In re Google Inc. Cookie Placement Consumer Priv. Litig.*,
 806 F.3d 125 (3d Cir. 2015)..... 21

25

26 *In re Google Inc. Gmail Litig.*,
 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013)..... 19, 23

27 *In re Google Location Hist. Litig.*,
 428 F. Supp. 3d 185 (N.D. Cal. 2019)..... *passim*

28

1 *In re Google, Inc. Privacy Pol’y Litig.*,
58 F. Supp. 3d 968 (N.D. Cal. 2014)..... 25

2

3 *Hammerling v. Google LLC*,
615 F. Supp. 3d 1069 (N.D. Cal. 2022)..... 14, 25, 27

4 *Hassler v. Sovereign Bank*,
374 F. App’x 341 (3d Cir. 2010)..... 9, 12

5

6 *Hazel v. Prudential Fin., Inc.*,
2023 WL 3933073 (N.D. Cal. June 9, 2023) 15

7

8 *Heeger v. Facebook, Inc.*,
2019 WL 7282477 (N.D. Cal. Dec. 27, 2019) 24

9 *Heeger v. Facebook, Inc.*,
509 F. Supp. 3d 1182 (N.D. Cal. 2020)..... 8, 23

10

11 *Hernandez v. Hillsides, Inc.*,
47 Cal. 4th 272 (2009)..... 24

12

13 *Hicks v. PGA Tour, Inc.*,
897 F.3d 1109 (9th Cir. 2018)..... 9, 17

14 *Hill v. Nat’l Collegiate Athletic Ass’n*,
7 Cal. 4th 1 (1994)..... 9, 22, 23

15

16 *Huynh v. Quora, Inc.*,
2019 WL 11502875 (N.D. Cal. Dec. 19, 2019) 15

17 *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*,
2007 WL 4394447 (E.D. Pa. Dec. 13, 2007) 21

18 *In re iPhone Application Litigation*,
844 F. Supp. 2d 1040 (N.D. Cal. 2012)..... 25

19

20 *Kearns v. Ford Motor Co.*,
567 F.3d 1120 (9th Cir. 2009)..... 7, 26

21

22 *Khoja v. Orexigen Therapeutics, Inc.*,
899 F.3d 988 (9th Cir. 2018)..... 7

23

24 *Kumandan v. Google LLC*,
2022 WL 103551 (N.D. Cal. Jan. 11, 2022) 28

25

26 *Kurowski v. Rush Sys. for Health*,
2023 WL 4707184 (N.D. Ill. July 24, 2023) 29

27 *Kwikset Corp. v. Super. Ct.*,
51 Cal. 4th 310 (2011)..... 29

28

1 *Lee v. Wells Fargo Bank, N.A.*,
 2013 WL 1117866 (N.D. Cal. Mar. 18, 2013) 16

2 *Lightoller v. Jetblue Airways Corp.*,
 3 2023 WL 3963823 (S.D. Cal. June 12, 2023) 8

4 *Low v. LinkedIn Corp.*,
 5 900 F. Supp. 2d 1010 (N.D. Cal. 2012)..... 16, 25

6 *Lugones v. Pete and Gerry’s Organic, LLC*,
 440 F. Supp. 3d 226 (S.D.N.Y. 2020) 27

7 *LVRC Holdings LLC v. Brekka*,
 8 581 F.3d 1127 (9th Cir. 2009)..... 20

9 *Mastel v. Miniclip SA*,
 10 549 F. Supp. 3d 1129 (E.D. Cal. 2021) 9, 18, 24

11 *McCoy v. Alphabet, Inc.*,
 2021 WL 405816 (N.D. Cal. Feb. 2, 2021)..... 25

12 *Mikulsky v. Noom, Inc.*,
 13 2023 WL 4567096 (S.D. Cal. July 17, 2023)..... 8

14 *Mladenov v. Wegmans Food Markets, Inc.*,
 15 124 F. Supp. 3d 360 (D.N.J. 2015)..... 27

16 *Mollaei v. Otonomo Inc.*,
 651 F. Supp. 3d 1135 (N.D. Cal. 2023)..... 18

17 *Moreno v. San Francisco Bay Area Rapid Transit Dist.*,
 18 2017 WL 6387764 (N.D. Cal. Dec. 14, 2017) 18

19 *Morrissey v Nextel Partners, Inc.*,
 20 72 A.D.3d 209 (N.Y. 2010)..... 27

21 *Naimi v. Starbucks Corp.*,
 798 F. App’x 67 (9th Cir. Dec. 20, 2019) 29

22 *Nguyen v. Stephens Inst.*,
 23 529 F. Supp. 3d 1047 (N.D. Cal. 2021)..... 16

24 *Oliveira v. Amoco Oil Co.*,
 776 N.E.2d 151 (Ill. 2002) 27

25 *Orlander v. Staples, Inc.*,
 26 802 F.3d 298 (2d Cir. 2015) 29

27 *People v. Drennan*,
 28 84 Cal. App. 4th 1349 (2000)..... 18, 20

1 *People v. Guzman*,
8 Cal. 5th 673 (2019)..... 17

2

3 *Popa v. Harriet Carter Gifts, Inc.*,
52 F.4th 121 (3d Cir. 2022)..... 20, 22

4 *Putian Authentic Enter. Mgmt. Co. v. Meta Platforms, Inc.*,
2022 WL 1171034 (N.D. Cal. Apr. 19, 2022)..... 14, 15

5

6 *Quigley v. Yelp, Inc.*,
2018 WL 7204066 (N.D. Cal. Jan. 22, 2018) 17, 20

7

8 *Randall v. Univ. of the Pac.*,
2022 WL 1720085 (N.D. Cal. May 28, 2022) 16

9 *Revitch v. New Moosejaw, LLC*,
2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) 20

10

11 *Riordan v. W. Digital Corp.*,
2023 WL 6462857 (N.D. Cal. Sept. 29, 2023)..... 30

12

13 *Rivera v. Invitation Homes, Inc.*,
2019 WL 11863726 (N.D. Cal. June 19, 2019) 22

14 *Rodio v. Smith*,
123 N.J. 345 (1991)..... 27

15

16 *Rodriguez v. Google LLC*,
2021 WL 2026726 (N.D. Cal. May 21, 2021) 20, 24

17

18 *Rudgayzer v. Yahoo! Inc.*,
2012 WL 5471149 (N.D. Cal. Nov. 9, 2012)..... 15

19 *S.D. v. Hytto Ltd.*,
2019 WL 8333519 (N.D. Cal. May 15, 2019) 21

20

21 *Salameh v. Tarsadia Hotel*,
726 F.3d 1124 (9th Cir. 2013)..... 26

22

23 *Schippell v. Johnson & Johnson Consumer Inc.*,
2023 WL 6178485 (C.D. Cal. Aug. 7, 2023) 16

24 *Shwarz v. United States*,
234 F.3d 428 (9th Cir. 2000)..... 13

25

26 *Silver v. Stripe, Inc.*,
2021 WL 3191752 (N.D. Cal. July 28, 2021) 9, 10, 12, 16

27 *Small v. Lorillard Tobacco Co.*,
94 N.Y.2d 43 (1999)..... 29

28

1 *Smith v. Facebook, Inc.*,
 262 F. Supp. 3d 943 (N.D. Cal. 2017)..... 10, 12, 17, 23

2 *Smith v. LoanMe, Inc.*,
 3 11 Cal. 5th 183 (2021)..... 20

4 *Solo v. Bed Bath & Beyond, Inc.*,
 5 2007 WL 1237825 (D.N.J. Apr. 26, 2007)..... 29

6 *Sonner v. Premier Nutrition Corp.*,
 7 971 F.3d 834 (9th Cir. 2020)..... 30

8 *Swarts v. Home Depot, Inc.*,
 2023 WL 5615453 (N.D. Cal. Aug. 30, 2023)..... 19

9 *Tabak v. Apple, Inc.*,
 10 2020 WL 9066153 (N.D. Cal. Jan. 30, 2020) 27, 28

11 *TBG Ins. Servs. Corp. v. Super. Ct.*,
 96 Cal. App. 4th 443 (2002)..... 19

12 *Tietsworth v. Sears, Roebuck & Co.*,
 13 2009 WL 3320486 (N.D. Cal. Oct. 13, 2009)..... 28

14 *United States v. Forrester*,
 15 512 F.3d 500 (9th Cir. 2008)..... 23, 24

16 *Valenzuela v. Keurig Green Mountain, Inc.*,
 2023 WL 6609351 (N.D. Cal. Oct. 10, 2023) 8

17 *White v. Samsung Elecs. Am., Inc.*,
 18 2019 WL 8886485 (D.N.J. Aug. 21, 2019)..... 29

19 *Williams v. What If Holdings, LLC*,
 20 2022 WL 17869275 (N.D. Cal. Dec. 22, 2022) 29

21 *In re Yahoo Mail Litig.*,
 7 F. Supp. 3d 1016 (N.D. Cal. 2014)..... 22

22 *Yari v. Producers Guild of Am., Inc.*,
 23 161 Cal. App. 4th 172 (2008)..... 14, 15

24 *Yoon v. Lululemon USA, Inc.*,
 25 549 F. Supp. 3d 1073 (C.D. Cal. 2021)..... 21, 23

26 *In re Zynga Priv. Litig.*,
 750 F.3d 1098 (9th Cir. 2014)..... 21

27

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Statutes

18 Pa. C.S. § 5702 20, 21

18 Pa. C.S. § 5703 20

15 U.S.C. § 6501(1)..... 6

Cal. Bus. & Prof. Code § 17200..... 26

Cal. Civ. Code § 3515 9

Cal. Penal Code § 632(a)..... 17

Ill. Comp. Stat. Ann. 505/1 26

N.J. Stat. Ann. § 56:8-1 26

N.Y. Gen. Bus. Law §§ 349, 350 26, 27

Other Authorities

Black’s Law Dictionary (11th ed. 2019) 9, 18

Fed. R. Civ. P. 9(b).....*passim*

1 **NOTICE OF MOTION/MOTION:** PLEASE TAKE NOTICE that on March 21, 2024, at 9:00
2 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
3 consolidated class action complaint. The motion is based on the memorandum, documents incorporated
4 by reference or judicially noticeable, and evidence and argument as the Court permits.

5 **MEMORANDUM IN SUPPORT: INTRODUCTION AND STATEMENT OF ISSUES**

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

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

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

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

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

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

8 STATEMENT OF FACTS

9 A. Apple Privacy Disclosures and App Data Collection.

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

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

24 ***Privacy Policy.*** Apple's Privacy Policy discloses that Apple may collect account, device, contact,
 25 and transaction data, including "[y]our Apple ID and related account details" and "[d]ata from which your
 26 device could be identified." RJN Ex. 3 (Privacy Policy) at 3. It explains that Apple may collect "[d]ata
 27

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

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

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

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

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

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

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

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

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

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

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

2 **C. The Allow Apps to Request to Track Setting.**

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

9 Apple’s setting descriptions and disclosures consistently explain its function. Directly below the
10 setting, it says: “Allow apps *to ask* to track your activity across *other companies’ apps and websites*.
11 When this is off, all new app tracking requests are automatically denied.” *See* RJN Ex. 16 (Allow Apps
12 to Request to Track setting screen) (emphasis added). A hyperlink leads to a Tracking disclosure with
13 more detail: “Apple requires app developers to *ask for permission* before they track your activity *across*
14 *apps or websites they don’t own*[.]” *See* RJN Ex. 17 (Tracking disclosure) at 1 (emphasis added); Compl.
15 ¶¶ 105-06. It goes on: “You can control whether apps can ask for permission to track your activity . . . If
16 you don’t want to be asked for your permission, or do not want apps to access your device’s Advertising
17 Identifier, you can disable Allow Apps to Request to Track.” RJN Ex. 17 (Tracking disclosure) at 3.
18 Similarly, the Privacy Policy explains, “If you disable Allow Apps to Request to Track, third-party apps
19 cannot request to use the Advertising Identifier . . . to track you across apps and websites *owned by other*
20 *companies*.” *See* RJN Ex. 3 (Privacy Policy) at 8 (emphasis added).

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

22 Apple does not permit children under the age of 13 to create their own Apple IDs. *See* RJN Ex.
23 18 (Family Privacy Disclosure for Children (“Family Disclosure”)) at 3. Instead, a parent or guardian
24 must create the account, as explained in the Family Disclosure and the incorporated Privacy Policy. *See*
25 *id.*; Ex. 3 (Privacy Policy) at 7. During the setup process, the parent is presented with the Family
26 Disclosure and “consent[s] to Apple’s collection, use, and disclosure of [the] child’s information as set
27 forth in Apple’s Privacy Policy and this Disclosure.” *See* RJN Ex. 18 (Family Disclosure) at 5. The
28 Family Disclosure explains that Apple “may collect things like device identifiers, cookies, IP addresses,

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

8 **E. Procedural History and Plaintiffs’ Allegations.**

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

13 Plaintiffs allege that they own iPhones, iPads, or Watches and “regularly use[] mobile applications
14 owned by Apple.” Compl. ¶¶ 11-25. Minor plaintiffs A.H. and E.M. do not say which apps they use, *id.*
15 ¶¶ 16, 24, while the other plaintiffs give examples, *see, e.g., id.* ¶¶ 23, 25. Plaintiffs allege that at some
16 unspecified date they turned off Allow Apps to Request to Track and/or Share [Device] Analytics on their
17 devices. *Id.* ¶¶ 11-25 While plaintiffs assert that “Apple accessed and recorded [plaintiffs’] data while
18 [they were] using Apple’s mobile applications,” *id.*, they do not identify what information Apple
19 purportedly “accessed” about them, from which apps, or what that information supposedly revealed.

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

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

1 performance statistics, and data about how they used their devices and applications tracked and/or
 2 collected by Apple while using an Apple app (e.g., App Store, Apple Music, Apple TV, Books, and
 3 Stocks) on their mobile Apple device (i.e., iPhone, iPad, or Apple Watch) with the ‘Allow Apps to Request
 4 to Track’ and/or ‘Share [Device] Analytics’ settings turned off.” *Id.* ¶¶ 85-91.³ Based on this class
 5 definition and the lack of any factual allegations about other apps, plaintiffs’ claims appear to be based
 6 only on App Store, Music, TV, Books, and Stocks.

7 LEGAL STANDARD

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

14 ARGUMENT

15 **I. Plaintiffs Have Not Established Standing or Stated a Claim Because They Allege No Facts 16 About Their Own Experiences.**

17 A complaint that does little more than “parrot[] internet musings about things [a defendant] may
 18 or may not be doing, and which plaintiffs may or may not have experienced themselves,” cannot survive
 19 dismissal. *Crittenden v. Apple, Inc.*, 2022 WL 2132224, at *4 (N.D. Cal. June 14, 2022). More than one
 20 year has passed since the initial complaint was filed, yet all plaintiffs offer to support their claims are press
 21 reports about a few of the apps they mention, speculation about what the alleged collection might reveal,
 22 and conclusory allegations that Apple “accessed and recorded” unspecified data when plaintiffs were
 23 using “mobile applications owned by Apple.” *See, e.g.*, Compl. ¶¶ 11-25, 51-56. Plaintiffs do not allege
 24 what data was collected from *them* or any facts about the collection practices of apps beyond those in their
 25
 26

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

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

4 Allegations about plaintiffs’ own experiences are particularly important for assessing Article III
5 standing for privacy claims because courts analyze concrete harm under the Supreme Court’s *TransUnion*
6 decision “based on the nature of the information at issue.” *See Mikulsky v. Noom, Inc.*, 2023 WL 4567096,
7 at *5 (S.D. Cal. July 17, 2023). Where plaintiffs do not allege what information was collected about *them*,
8 courts routinely dismiss claims for lack of concrete harm under Article III. In *Valenzuela v. Keurig Green*
9 *Mountain, Inc.*, for example, the plaintiff claimed that her privacy was invaded when her conversation
10 with a website’s customer service chat feature was recorded. 2023 WL 6609351, at *1 (N.D. Cal. Oct.
11 10, 2023). The court held that, without “any information at all about the contents of the chat,” the plaintiff
12 had alleged only “a bare procedural violation, divorced from any concrete harm.” *Id.* at *2. Similarly, in
13 *Lightoller v. Jetblue Airways Corp.*, allegations that third-party software collected “clicks, keystrokes
14 (such as text being entered into an information field or text box), [and] URLs of webpages visited” were
15 insufficient to allege concrete harm. 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023).

16 The same result follows here. Plaintiffs allege that some apps collect data about clicks or searches,
17 Compl. ¶ 52, but they do not provide any facts about what data was collected from *them* or what that data
18 supposedly revealed. *See also Cook v. GameStop, Inc.*, 2023 WL 5529772, at *4-5 (W.D. Pa. Aug. 28,
19 2023) (no standing where plaintiff did not allege what her clicks or browsing history revealed about her);
20 *Mikulsky*, 2023 WL 4567096, at *4-5 (same for website chat feature); *Byars v. Sterling Jewelers, Inc.*,
21 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023) (same); *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d
22 1182, 1188 (N.D. Cal. 2020) (no standing where plaintiffs did not identify any sensitive collected data).

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

25
26 ⁴ To the extent plaintiffs seek to broaden their claims to other apps, their own sources contradict them
27 and weigh further in support of dismissal. *See id.* ¶¶ 53, 56 (citing Gizmodo articles); *Crittenden*, 2022
28 WL 2132224, at *3 (citing contradictory evidence in materials plaintiffs invoked as basis for dismissal).

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

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

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

16 “[A] person is not wronged by that to which he or she consents[.]” Black’s Law Dictionary (11th
 17 ed. 2019) (defining “volenti non fit injuria”); Cal. Civ. Code § 3515 (plaintiff “who consents to an act is
 18 not wronged by it”). As a result, courts routinely dismiss claims where, as here, the plaintiffs’ conduct
 19 manifested consent under applicable law. *See, e.g., Hill v. Nat’l Collegiate Athletic Ass’n*, 7 Cal. 4th 1,
 20 26 (1994) (plaintiff “must not have manifested by his or her conduct a voluntary consent” to alleged
 21 privacy violation); *Silver v. Stripe, Inc.*, 2021 WL 3191752, at *4-5 (N.D. Cal. July 28, 2021) (consent via
 22 privacy disclosures defeated CIPA claims); *see also Hicks v. PGA Tour, Inc.*, 897 F.3d 1109, 1120 n.6
 23 (9th Cir. 2018) (affirming dismissal of unjust enrichment claim based on consent); *Hassler v. Sovereign*
 24 *Bank*, 374 F. App’x 341, 344 (3d Cir. 2010) (New Jersey Consumer Fraud Act (“NJCFA”) claim failed
 25 where account agreement “clearly explained” the challenged actions); *Calhoun v. Google, LLC*, 645 F.
 26 Supp. 3d 916, 928 (N.D. Cal. 2022) (consent a defense to contract, implied covenant, and UCL claims).

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

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

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

5 Here, plaintiffs allege that Apple "secretly" collects "details about app usage, app browsing
6 communications, personal information, and information relating to the mobile device itself" through
7 "Apple's proprietary applications." Compl. ¶¶ 1, 4, 50. Like in *Smith*, Apple disclosed this exact
8 collection, barring plaintiffs' claims. Take the App Store as an example. Plaintiffs assert that the App
9 Store collects "what was tapped on, which Apps were searched for, what ads were displayed, how long
10 an app was viewed, and how the app was found," as well as "device identification numbers, what kind of
11 device was used, the device's screen resolution, the device's keyboard language, and how the user was
12 connected to the internet." Compl. ¶ 52. All of this was disclosed to plaintiffs, and they agreed to the
13 collection by assenting to the software license agreement and using the apps.

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

18 The Privacy Policy discloses that Apple may collect the types of data plaintiffs complain of here,
19 including "[d]ata about your activity on and use of our offerings, such as app launches within our services,
20 including browsing history; search history; product interaction; crash data, performance and other
21 diagnostic data; and other usage data." *See* RJN Ex. 3 (Privacy Policy) at 3; Compl. ¶¶ 2, 48, 103, 134,
22 141 (relying on Privacy Policy). The Privacy Policy also discloses that collection may include "[d]ata
23 from which your device could be identified, such as device serial number, or about your device, such as
24 browser type." *See* RJN Ex. 3 (Privacy Policy) at 3.

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

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

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

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

Complaint’s Allegation	App Store & Privacy Disclosure
<p>13 App store collects “what was tapped on, which Apps were searched for, what ads 14 were displayed, how long an app was viewed, and how the app was found.” 15 Compl. ¶ 52.</p>	<p>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.</p> <p>“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.” <i>Id.</i></p> <p>“The information Apple receives about your usage of the stores includes information about the personalized content you tap and view.” <i>Id.</i></p>
<p>22 App Store collects “details about a user’s mobile device . . . , including 23 device identification numbers, what kind of device was used, the device’s 24 screen resolution, the device’s keyboard language, and how the user was 25 connected to the internet.” Compl. ¶ 52.</p>	<p>“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.</p> <p>“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.” <i>Id.</i> at 2.</p>

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

1 choose whether an app can track your activity *across other companies' Apps and websites for the purposes*
 2 *of advertising or sharing with data brokers.*” *Id.* ¶ 44 (emphasis added). That same support page defines
 3 “tracking” as occurring “when information that identifies you or your device collected from an app is
 4 linked with information that identifies you or your device *collected on apps, websites and other locations*
 5 *owned by third parties[.]*” *See If an app asks to track your activity*, APPLE (Feb. 13, 2023),
 6 <https://support.apple.com/en-us/HT212025> (emphasis added) (cited in Compl. ¶ 44). Plaintiffs also
 7 include a screen shot of the Tracking disclosure, which explains that Apple “requires app developers to
 8 ask for permission before they track your activity *across Apps or websites they don't own.*” Compl. ¶ 105.

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

18 2. “Share [Device] Analytics” Does Not Control the Data Collection at Issue.

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

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

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

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

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

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

15 Plaintiffs cannot establish the required element of breach, which warrants dismissal of the contract,
16 implied contract, and implied covenant claims. *See Hammerling v. Google LLC*, 615 F. Supp. 3d 1069,
17 1095 (N.D. Cal. 2022) (“Plaintiffs cannot state a claim for breach of contract without alleging a promise
18 that is breached.”); *see also Yari v. Producers Guild of Am., Inc.*, 161 Cal. App. 4th 172, 182 (2008)
19 (implied contract); *Putian Authentic Enter. Mgmt. Co. v. Meta Platforms, Inc.*, 2022 WL 1171034, at *7
20 (N.D. Cal. Apr. 19, 2022) (implied covenant). Unable to identify any breach of the software licenses or
21 Privacy Policy, plaintiffs contend that the alleged contract “incorporates the mobile device’s settings into
22 the terms of the parties’ agreement.” Compl. ¶ 103. That argument does not save plaintiffs’ claims
23 because the settings govern other types of collection not at issue here. *See supra*, Section II.B.

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

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

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

15 **B. The Complaint Does Not Plausibly Plead Damages.**

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

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

24 Plaintiffs’ conclusory contention that “the value of their data” decreased fares no better. Compl.
 25 ¶¶ 118, 128, 137. While plaintiffs allege that data has value to companies, that does not show any loss to
 26 plaintiffs. *See, e.g., id.* ¶¶ 60, 63-65; *Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *6 (N.D. Cal.
 27 June 9, 2023). They claim that other companies’ studies paid users to monitor their web-browsing, Compl.
 28 ¶¶ 69-71, or that platforms allow users to “own and earn from their data,” *id.* ¶ 77, but they do not allege

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

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

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

18 Plaintiffs’ implied contract and unjust enrichment claims also should be dismissed because
19 plaintiffs contend an express contract governs the subject. As this Court has explained, “there cannot be
20 a valid, express contract *and* an implied contract, each embracing the same subject matter, existing at the
21 same time.” *Randall v. Univ. of the Pac.*, 2022 WL 1720085, at *4 (N.D. Cal. May 28, 2022); *Nguyen v.*
22 *Stephens Inst.*, 529 F. Supp. 3d 1047, 1056-57 (N.D. Cal. 2021) (same for unjust enrichment).

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

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

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

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

4 Section 632, enacted in 1967, prohibits “intentionally and without the consent of all parties to a
5 confidential communication, us[ing] an electronic amplifying or recording device to eavesdrop upon or
6 record the confidential communication.” Cal. Penal Code § 632(a). To address advances in technology,
7 the legislature in 1985 passed Section 632.5 to ensure that CIPA applied to a new technology at that time:
8 cellular phones. *See People v. Guzman*, 8 Cal. 5th 673, 687 (2019). In 1990, it amended CIPA to address
9 another new technology: cordless telephones. *Id.* at 689. Other provisions of CIPA have been amended
10 to account for body-worn cameras, § 633.02(b) (added in 2016); the distribution of confidential health
11 care communications on the internet, § 632.01(a)(1) (2016); satellite television, § 637.5 (1982); and
12 rideshare programs, § 637.6 (1990). Despite multiple changes to account for other technologies, the
13 legislature has not amended CIPA to include data collection. Instead, in 2018, it passed the California
14 Consumer Privacy Act, which comprehensively regulates collection and use of consumers’ personal data.

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

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

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

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

1 that the apps here do not qualify as an “amplifying or recording device.” In *Google Location History* and
2 *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *5 (N.D. Cal. Dec. 14,
3 2017), the courts considered whether apps were “location tracking devices” within the meaning of Section
4 637.7 and concluded they were not. The courts explained that software is not a “device” within the
5 meaning of the statute because it is not “equipment” made for the specific purpose of location tracking.
6 *Google Location Hist.*, 428 F. Supp. 3d at 193-94 (Google Maps app is software, not a “device”); *Moreno*,
7 2017 WL 6387764, at *5 (same for BART app). The same result follows here. These apps are software
8 designed to provide users with music, information about stocks, or access to other apps. They are not
9 “equipment” primarily designed to “amplify or record.” *Cf. Mollaei v. Otonomo Inc.*, 651 F. Supp. 3d
10 1135, 1140-41 (N.D. Cal. 2023) (following *Google Location History* and *Moreno* to find that an integrated
11 vehicle component was not an “electronic tracking device”); *Mastel*, 549 F. Supp. 3d at 1135 (declining
12 to interpret “telephone device” to include the iOS Pasteboard).

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

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

15 *Fifth*, plaintiffs fail to allege that their data is a confidential communication within the meaning of
16 Section 632. “Confidential communication” is defined as a communication “in circumstances as may
17 reasonably indicate that any party to the communication desires it to be confined to the parties thereto,”
18 but excludes circumstances where the parties “may reasonably expect that the communication may be . . .
19 recorded.” § 632(c). Given Apple’s extensive privacy disclosures, no reasonable user would expect that
20 their actions in Apple’s apps would be private from Apple. *See Swarts v. Home Depot, Inc.*, 2023 WL
21 5615453, at *8 (N.D. Cal. Aug. 30, 2023) (allegation that consumers “cannot be expected to know that
22 chat conversations with customer service agents are generally recorded is objectively unreasonable”).

23 Moreover, while phone conversations often are found to be confidential if a party has no reason to
24 believe someone else is listening in, California courts generally presume that written electronic
25 communications “are not ‘confidential’ within the meaning of [S]ection 632,” because they “can easily be
26 shared by, for instance, the recipient(s).” *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal.
27 2014). Plaintiffs do not allege any facts about their app use, so they cannot establish that any
28 communications were “confidential” within the meaning of section 632, let alone overcome the

1 presumption to the contrary. *See Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1020 (9th Cir. 2013)
2 (allegation that plaintiff called to dispute a charge not enough detail about the context to establish an
3 objectively reasonable expectation of confidentiality); *Rodriguez v. Google LLC*, 2021 WL 2026726, at
4 *7 (N.D. Cal. May 21, 2021) (sensitivity of users’ online queries and browsing histories did not make data
5 “confidential” under Section 632); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal.
6 Oct. 23, 2019) (“browsing activity and form field entries” on a website not confidential communications).

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

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

18 WESCA is Pennsylvania’s statute that “operates in conjunction with and as a supplement to the
19 Federal Wiretap Act.” *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125-26 (3d Cir. 2022). As relevant
20 here, it prohibits the intentional interception of the contents of any electronic communication. 18 Pa. C.S.
21 § 5703. Plaintiffs fail to allege any of the elements of an unlawful interception claim under WESCA.

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

24 *Second*, plaintiffs do not allege an “interception” under WESCA because Apple did not obtain the
25 “contents” of any “communication.” WESCA defines “contents” as “any information concerning the
26 substance, purport, or meaning of that communication.” 18 Pa. C.S. § 5702. This definition is identical
27 to the Federal Wiretap Act’s definition of “contents,” and identical terms in the two statutes are
28 “interpreted in the same way.” *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 n.6 (3d Cir. 2003).

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

5 Plaintiffs have not alleged the collection of “content” within the meaning of WESCA. They assert
6 that Apple collects “what was tapped on, which Apps were searched for, what ads were displayed, how
7 long an app was viewed, and how the app was found,” as well as “details about a user’s mobile device.”
8 Compl. ¶¶ 52, 186. This information does not constitute “the substance, purport, or meaning”—*i.e.*, the
9 “contents”—of communications under WESCA; rather, it is “record information” describing how a user
10 interacts with the apps. *See Zynga*, 750 F.3d at 1106; *see also S.D. v. Hytto Ltd.*, 2019 WL 8333519, at
11 *6 (N.D. Cal. May 15, 2019) (under the Federal Wiretap Act, “the origin of a phone call, a phone call’s
12 length, and geolocation data from an app,” as well as the “date and time of usage data” collected are not
13 “content,” but “record information”); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082-83 (C.D.
14 Cal. 2021) (clicks, pages visited, keystrokes, and PII, including shipping and billing information, are not
15 “contents” under California’s analogous wiretap statute).

16 *Third*, plaintiffs fail to plausibly allege collection by a “device,” as required to state a claim. *Ideal
17 Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, at *4 (E.D. Pa. Dec. 13, 2007). WESCA
18 defines a “device” as “[a]ny device or apparatus . . . that can be used to intercept a wire, electronic or oral
19 communication.” 18 Pa. C.S. § 5702. However, the device performing the alleged interception must be
20 separate from the source of the communication. *See Commonwealth v. Diego*, 119 A.3d 370, 374 (Pa.
21 Super. 2015) (finding that an iPad from which the intercepted communication originated was not the
22 relevant device). Here, plaintiffs allege that their mobile devices are the intercepting devices under
23 WESCA, Compl. ¶ 185, and also the sources of the purportedly intercepted communications. *Id.* ¶¶ 1, 11-
24 25 (stating that Apple collects “users’ data when they interact with Apple’s proprietary applications . . .
25 on their mobile Apple devices”). That is fatal to their WESCA claims. *See Diego*, 119 A.3d at 374.

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

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

2 Plaintiffs' citation to the Third Circuit's decision in *Popa*, 52 F.4th at 124, does not change the
 3 result. That decision is not binding on this court, *see Rivera v. Invitation Homes, Inc.*, 2019 WL 11863726,
 4 at *2 (N.D. Cal. June 19, 2019), and diverges from the Pennsylvania state court decisions that have
 5 consistently recognized the direct-party exception. *See Commonwealth v. Cruttenden*, 58 A.3d 95, 98-
 6 100 (Pa. 2012); *Proetto*, 771 A.2d at 831; *Diego*, 119 A.3d at 380-81. Moreover, *Popa* does not apply on
 7 its facts. There, the court stated that the plaintiff "obviously knew" her browser was communicating with
 8 the website she was viewing (operated by defendant) but did not know that her browser was *also*
 9 communicating with a third-party marketing company. *Popa*, 52 F.4th at 124. Here, plaintiffs "obviously
 10 knew" they were interacting with Apple when using Apple's apps and do not allege that any data was
 11 transmitted to any third party. Under these facts, *Popa* does not apply.

12 **C. Apple Did Not Invade Plaintiffs' Privacy.**

13 Apple believes that privacy is a fundamental human right and designs its products and services
 14 with privacy in mind. The allegations plaintiffs advance here do not support their claims for violations of
 15 the California constitutional privacy right. "The California Constitution sets a 'high bar' for establishing
 16 an invasion of privacy claim." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014).
 17 Plaintiffs must plead (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the
 18 circumstances; and (3) a serious invasion of privacy constituting "an egregious breach of . . . social
 19 norms." *Hill*, 7 Cal. 4th at 35-37. The complaint's sparse allegations do not satisfy these elements.

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

21 California law recognizes two classes of legally protected privacy interests: (1) informational
 22 privacy, which is the interest in "precluding the dissemination or misuse of sensitive and confidential
 23 information," and (2) autonomy privacy, which is the interest in "making intimate personal decisions or
 24 conducting personal activities without observation, intrusion, or interference." *Google Location Hist.*,
 25 428 F. Supp. 3d at 196-97. The complaint's limited facts do not satisfy either.

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

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

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

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

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

22 *Second*, plaintiffs cannot reasonably expect that data they knowingly provide to Apple would not
23 be received by Apple. In *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), for example, the Ninth
24 Circuit held that internet users do not have a reasonable expectation of privacy in the to/from addresses of
25 e-mail messages or the IP addresses of websites visited “because they should know that this information
26 is provided to and used by Internet service providers for the specific purpose of directing the routing of
27 information.” *Id.* at 510; *see also Heeger*, 509 F. Supp. 3d at 1189-90 (same). The same is true here.
28 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*

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

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

12 3. Disclosed Data Collection Is Not an “Egregious Breach” of Social Norms.

13 The privacy claim also fails to state the third element: that the alleged collection is “so serious ‘in
14 nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.’”
15 *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009). Courts regularly dismiss claims under this
16 element where the plaintiffs do not plead facts showing that the data collected from them was sensitive.
17 For example, in *Mastel*, the plaintiff alleged that an app secretly accessed the iPhone’s Pasteboard, which
18 allows users to copy text between apps. 549 F. Supp. 3d at 1132-33. The Pasteboard allegedly may have
19 contained “his contact information, addresses for his friends and relatives, or text from messages that he
20 had sent.” The court found that accessing such information was not an egregious breach without any
21 allegation the information was sensitive. *See id.* at 1141-42; *see also Heeger v. Facebook, Inc.*, 2019 WL
22 7282477, at *4 (N.D. Cal. Dec. 27, 2019) (conclusory allegation that defendant accessed “private” location
23 data insufficient). Here, the complaint’s sole allegation about plaintiffs’ app use is that they “regularly
24 use[] mobile applications owned by Apple.” Compl. ¶¶ 11-25. The complaint says nothing about what
25 information Apple allegedly gathered about plaintiffs, let alone why any such information was sensitive.

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

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

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

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

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

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

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

7 **A. The Misrepresentation Theory Is Not Adequately Alleged.**

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

12 Plaintiffs' core theory in each of the consumer-protection claims is that the Allow Apps to Request
 13 to Track and Share [Device] Analytics settings "promised that they would prevent Plaintiffs' and the
 14 Class's user data from being collected while they used an Apple device." Compl. ¶ 104; *see also id.* ¶¶ 1,
 15 5, 49, 50, 165, 246, 265. But the complaint does not identify *any* statement by Apple actually saying that.
 16 Instead, the Privacy Policy and service-specific disclosures expressly disclose the complained-of
 17 collection. Moreover, the settings and related disclosures specify that they govern (1) requests to track
 18 across third-party apps/websites, and (2) certain device performance data, neither of which is at issue here.

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

24 **No reliance.** Rule 9(b) requires plaintiffs to specify when they were exposed to the purported
 25 misleading statements and whether they relied on them. *Kearns*, 567 F.3d at 1126. Here, seven plaintiffs
 26 do not allege ever seeing or relying on any statement by Apple. *See* Compl. ¶¶ 11, 14, 16, 17, 21, 22, 24.
 27 While the other six plaintiffs allege generally relying on privacy-related advertising, *id.* ¶¶ 12, 13, 15, 18,
 28 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.

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

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

6 *Second*, Rule 9(b) requires plaintiffs to allege with particularity that, had Apple made specific
7 disclosures, plaintiffs would have been aware of them and would not have purchased their devices. *See*
8 *Tabak*, 2020 WL 9066153, at *9; *cf. Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1225 (9th Cir. 2015)
9 (plaintiffs must show “that, had the omitted information been disclosed, one would have been aware of it
10 and behaved differently”). In *Tabak*, for example, plaintiffs alleged they “would not have purchased the
11 devices at issue if they had known about the defect.” 2020 WL 9066153, at *9. The court found these
12 allegations “lack[ed] specific factual matter to raise the reasonable inference that, had Apple disclosed
13 information about the defect, Plaintiffs ‘would have been aware of it and behaved differently.’” *Id.* Here,
14 plaintiffs assert, without factual support, that they “would not have purchased their devices from [Apple]
15 or would have paid less for them” had they known about the alleged data collection. *See* Compl. ¶¶ 171,
16 209, 232, 249, 269. These allegations are indistinguishable from those in *Tabak*.

17 *Third*, the complaint does not identify a legal basis for any duty to disclose. *See, e.g., Eidmann v.*
18 *Walgreen Co.*, 522 F. Supp. 3d 634, 646-47 (N.D. Cal. 2021) (UCL); *Gold v. Lumber Liquidators, Inc.*,
19 2015 WL 7888906, at *11 (N.D. Cal. Nov. 30, 2015) (GBL, ICFA); *Arcand v. Brother Int’l. Corp.*, 673
20 F. Supp. 2d 282, 297 (D.N.J. 2009) (NJCFCA). A duty to disclose exists only when a defendant (1) is the
21 plaintiff’s fiduciary, (2) has exclusive knowledge of material facts not known to the plaintiff, (3) actively
22 conceals a material fact from the plaintiff, or (4) makes misleading partial representations. *Eidmann*, 522
23 F. Supp. 3d at 646. Plaintiffs have not alleged facts going to any of these scenarios. *See Tietsworth v.*
24 *Sears, Roebuck & Co.*, 2009 WL 3320486, at *4, *8 (N.D. Cal. Oct. 13, 2009) (no duty based on
25 “conclusory” allegations of “exclusive knowledge” and “active concealment”).

26 **C. Plaintiffs Do Not Allege Cognizable Damages.**

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

1 (7th Cir. 2014) (ICFA requires “actual damages”); *Small v. Lorillard Tobacco Co.*, 94 N.Y.2d 43, 56
 2 (1999) (GBL requires “either pecuniary or ‘actual’ harm”); *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310,
 3 323 (2011) (UCL requires “lost money or property”); *Solo v. Bed Bath & Beyond, Inc.*, 2007 WL 1237825,
 4 at *3 (D.N.J. Apr. 26, 2007) (NJCFRA requires “ascertainable loss of moneys or property”).

5 Plaintiffs allege that Apple “deprived Plaintiffs and Class Members of the economic value of their
 6 user data.” Compl. ¶ 84. That theory fails for the reasons explained in Section III.B. And an invasion of
 7 privacy, even if that had occurred here, is insufficient to establish “compensable damages” for the relevant
 8 claims. *See Williams v. What If Holdings, LLC*, 2022 WL 17869275, at *4 (N.D. Cal. Dec. 22, 2022)
 9 (alleged unauthorized recording of data does not establish injury under UCL); *see also Kurowski v. Rush*
 10 *Sys. for Health*, 2023 WL 4707184, at *6 (N.D. Ill. July 24, 2023) (invasion of privacy not “actual
 11 damages” under ICFA); *White v. Samsung Elecs. Am., Inc.*, 2019 WL 8886485, at *3-4 (D.N.J. Aug. 21,
 12 2019) (acquisition of personal data without consent not an ascertainable loss under NJCFRA); *Cohen*, 2018
 13 WL 3392877, at *7-9 (alleged privacy invasion not a cognizable injury under GBL).

14 Plaintiffs also allege without elaboration that they would not have used the Apple apps or
 15 purchased their devices, or would have paid less for their devices. *See* Compl. ¶¶ 171, 208-09, 231-32,
 16 248-49, 268-69. Conclusory allegations of overpayment do not allege cognizable damages under the
 17 consumer protection laws. *See Naimi v. Starbucks Corp.*, 798 F. App’x 67, 70 (9th Cir. Dec. 20, 2019)
 18 (GBL); *Camasta*, 761 F.3d at 739-40 (ICFA); *Gerritsen v. FCA US LLC*, 2020 WL 3841304, at *1 (C.D.
 19 Cal. Mar. 3, 2020) (UCL); *White*, 2019 WL 8886485, at *3 (NJCFRA). The price premium theory also
 20 fails because plaintiffs cannot have paid a premium for features they do not allege being aware of before
 21 purchase. *See supra*, Section III.B. Moreover, Allow Apps to Request to Track was introduced in 2021,
 22 *after* many plaintiffs bought their devices. Finally, the damages allegations also are deficient for the GBL
 23 claim to the extent they (1) seek to recover the entire purchase price, or (2) duplicate the contract damages
 24 plaintiffs seek. *See Orlander v. Staples, Inc.*, 802 F.3d 298, 302 (2d Cir. 2015); *Small*, 94 N.Y. 2d at 56.

25 **D. None of the California UCL Prongs Are Satisfied.**

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

1 predicated on same allegations as other failed claims). While plaintiffs refer to COPPA in passing, Compl.
 2 ¶ 165(f), merely listing laws, without alleging facts showing how a defendant violated them, does not
 3 state an “unlawful” claim. *See Doe v. CVS Pharmacy, Inc.*, 982 F.3d 1204, 1214 (9th Cir. 2020).

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

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

12 The existence of an adequate legal remedy deprives a court of equitable jurisdiction. *Sonner v.*
 13 *Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020). Plaintiffs thus “must plead inadequate legal
 14 remedies” to pursue UCL or unjust enrichment claims. *See, e.g., Riordan v. W. Digital Corp.*, 2023 WL
 15 6462857, at *9 (N.D. Cal. Sept. 29, 2023) (dismissing UCL claim under *Sonner*); *Apple Processor Litig.*,
 16 2022 WL 2064975, at *11-12 (same for unjust enrichment). Here, the complaint seeks the legal remedy
 17 of damages under CIPA, WESCA, and GBL. Compl. ¶¶ 148, 159, 192, 216, 239. The Court thus lacks
 18 equitable jurisdiction. Plaintiffs attempt to avoid dismissal of the equitable claims by contending that
 19 (1) legal remedies are not as certain and prompt as equitable relief, and (2) the Court may award restitution
 20 even if plaintiffs do not prove their legal claims. *See id.* ¶ 287. Those assertions misunderstand the
 21 inquiry—the question is not whether the elements of the legal and equitable claims differ, but rather
 22 whether the legal claims adequately can remedy any alleged harm. Since plaintiffs identify no reason the
 23 legal claims are inadequate, the UCL and unjust enrichment claims cannot proceed.

24 **CONCLUSION**

25 For the reasons stated, the complaint should be dismissed with prejudice.
 26
 27
 28

1 Dated: December 8, 2023

Respectfully submitted,

2 /s/ Kathryn E. Cahoy

3 Emily Johnson Henn (Bar No. 269482)
4 Kathryn E. Cahoy (Bar No. 298777)
5 COVINGTON & BURLING LLP
6 3000 El Camino Real
7 5 Palo Alto Square, 10th Floor
8 Palo Alto, CA 94306-2112
9 Telephone: (650) 632-4700
10 Facsimile: (650) 632-4800
11 Email: ehenn@cov.com
12 Email: kcahoy@cov.com

13 Amy S. Heath (Bar No. 312516)
14 COVINGTON & BURLING LLP
15 Salesforce Tower
16 415 Mission Street, Suite 5400
17 San Francisco, CA 94105-2533
18 Telephone: (415) 591-7030
19 Facsimile: (415) 955-6530
20 Email: aheath@cov.com

21 Attorneys for Defendant Apple Inc.