UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MICHAEL KATZ-LACABE, et al.,

Plaintiffs,

v.

ORACLE AMERICA, INC.,

Defendant.

Case No. 22-cv-04792-RS

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

I. INTRODUCTION

Three individual plaintiffs bring this putative class action against Oracle America, Inc. ("Defendant" or "Oracle"), alleging the company violates internet users' right to privacy, as provided under the California Constitution and various state and federal privacy statutes. Defendant moves to dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) for lack of standing and failure to state a claim, as well as failure to comply with Federal Rule of Civil Procedure 8. In addition, Oracle moves for an order striking portions of the Complaint pursuant to Federal Rule of Civil Procedure 12(f), as well as for judicial notice of several documents in support of its motion to dismiss. For the reasons that follow, the request for judicial notice is granted in part and denied in part; the motion to dismiss is granted in part and denied in part; and the motion to strike is denied.

II. BACKGROUND[1]

[1] The factual background is based on the well-pled allegations in the complaint, which are taken as true for the purposes of this motion.

Plaintiffs in this case are three named individuals—Michael Katz-Lacabe, a resident of San Leandro, California; Dr. Jennifer Golbeck, a resident of Sugarloaf Key, Florida; and Dr. Johnny Ryan, a resident of Dublin, Ireland—who purportedly represent five separate classes of individuals in a suit against Oracle. Plaintiffs' Complaint alleges that, "despite taking precautions to keep [their] personal information" private, Plaintiffs received a document from Oracle indicating that the company had tracked, compiled, and analyzed their web browsing and other activity, thereby creating an "electronic profile" on them. Dkt. 1 at 2-4.

Plaintiffs take issue with Oracle's extensive data brokering business—and in particular, two key features of Defendant's data management platform (BlueKai Data Management Platform): (1) the Oracle Data Marketplace, allegedly one of the world's largest commercial data exchanges; and (2) the Oracle ID Graph, a product designed to "match[] individual customer identities . . . and combin[e] them into a single consistent and accurate customer profile." Dkt. 1 at 7. According to Plaintiffs, Defendant's business model proceeds as follows: first, it collects as many types of personal information from internet users as possible. Then Defendant synchronizes that data to create individual profiles, and ultimately sells that data—bolstered by data made available by its partners—on its Data Marketplace.

A. Oracle's Alleged Data Collection

As Plaintiffs explain, Defendant's vast data accumulation is made possible by both Defendant's own technologies and the acquisition of data from other parties. In the former category, Defendant employs seven technologies, including: (1) cookies (pieces of software code stored on web browsers that collect users' data, like IP addresses); (2) the javascript code "bk-coretag.js" (proprietary code which copies and sends to Oracle what information users are requesting from a website server, such as a URL, date and time of visit, and webpage keywords); (3) tracking pixels (code embedded into webpages that track information whenever the webpage is opened); (4) device identification; (5) cross-device tracking; (6) AddThis widgets; and (7) Datalogix (an information broker specializing in profiles built from brick and mortar purchases). Allegedly "ubiquitous throughout the Internet," this data collection requires no relationship

between the internet user and Oracle to occur. Given this lack of privity, users "may not know Oracle is amassing data about them." Dkt. 1 at 12.

Defendant next uses its Oracle ID Graph to aggregate and synchronize the collected data to perform "identity resolution." This process takes three steps: (1) filtering and combining data from its various sources to identify and establish "a single, universal view of identity" for each user, across devices and marketing channels; (2) applying analytics to that raw data to develop insights about users and create segments along dimensions such as life events (e.g., marriage), education, purchase history, or even health and wellness (e.g., weight, sleep habits, and categories like "Aging & Geriatrics" and "Pain Relief"); and (3) matching data provided by customers to existing profiles that Defendant has developed and maintains in its Oracle Data Cloud, which helps "knit together" information from Defendant's own data sources.

Finally, Plaintiffs allege that Defendant's Data marketplace "is an online store owned and operated by Oracle where Oracle facilitates the buying and selling of data and data-derived services by Oracle" and its partners. Dkt. 1 at 26. This Marketplace trades in personal data Oracle collects itself, personal data that private companies collect from their own users and sell directly to Oracle's clients, and personal data that other third-party data brokers collect and sell to Oracle clients on the Marketplace. Defendant partners with over sixty-five "major brokers of third party data" in the Database, which allows it to profit from the sale of allegedly sensitive personal information including race, location, politics, and medical information. *Id.* at 33. With all of the available data, Defendant's products allow its clients to "analyze, segment, and target" users based on the information, including the categories of sensitive information outlined above.

B. Defendant's Privacy Policies & Plaintiffs' Lack of Consent

Plaintiffs further allege that neither Oracle's privacy policies, nor the policies of internet publishers, could provide any basis for Plaintiffs to have consented to the extensive data collection and profiling scheme described. Oracle's website leads to seven different privacy policies, which Plaintiffs describe as "convoluted, opaque, and not reasonably comprehensible to the average Internet user," Dkt. 1 at 43, and which Plaintiffs attack as failing to disclose what Oracle does with

internet users' information in any meaningful way. By way of example, Plaintiffs point to the Oracle Advertising Privacy Policy, which states that "Oracle does not create any online interest segments that reflect personal information that is sensitive," and includes in the category of sensitive information "certain aspects linked to personal life, such as racial or ethnic, religious, political, citizenship, immigration status, or sexual orientation." Dkt. 1 at 44; Oracle Advertising Privacy Policy, https://www.oracle.com/legal/privacy/advertising-privacy-policy.html. Plaintiffs allege that Defendant's practices are actually contrary to the reasonable reader's inference, from reading the policy, that Oracle would not facilitate the sale of their political views.

III. LEGAL STANDARD

Article III of the U.S. Constitution authorizes the judiciary to adjudicate only "cases" and "controversies." The doctrine of standing is "an essential and unchanging part of the case-or-controversy requirement of Article III." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). Defendant moves to dismiss on the basis that Plaintiffs lack standing under Rule 12(b)(1) of the Federal Rules of Civil Procedure. A 12(b)(1) motion to dismiss a complaint challenges the court's subject matter jurisdiction over the asserted claims. It is the plaintiff's burden to prove jurisdiction at the time the action is commenced. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016).

"A Rule 12(b)(1) jurisdictional attack may be facial or factual." *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). "In a facial attack, the challenger asserts that the allegations contained in the complaint are insufficient on their face to invoke federal jurisdiction." *Id.* Accordingly, when considering this type of challenge, the court is required to "accept as true the allegations of the complaint." *U.S. ex rel. Lujan v. Hughes Aircraft Co.*, 243 F.3d 1181, 1189 (9th Cir. 2001). However, "the district court is not restricted to the pleadings, but may review any evidence, such as affidavits and testimony, to resolve factual disputes concerning the existence of jurisdiction." *McCarthy v. United States*, 850 F.2d 558, 560 (9th Cir. 1988).

Defendant also alleges that Plaintiffs fail to state a claim. A complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). While "detailed factual allegations" are not required, a complaint must have sufficient

factual allegations to state a claim that is "plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 570 (2007)). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S. at 556). This standard asks for "more than a sheer possibility that a defendant has acted unlawfully." *Id.* The determination is a context-specific task requiring the court "to draw on its judicial experience and common sense." *Id.* at 679.

A Rule 12(b)(6) motion to dismiss tests the sufficiency of the claims alleged in the complaint. Dismissal under Rule 12(b)(6) may be based on either the "lack of a cognizable legal theory" or on "the absence of sufficient facts alleged under a cognizable legal theory." *See Conservation Force v. Salazar*, 646 F.3d 1240, 1242 (9th Cir. 2011) (internal quotation marks and citation omitted). When evaluating such a motion, the court must accept all material allegations in the complaint as true and construe them in the light most favorable to the non-moving party. *In re Quality Sys., Inc. Sec. Litig.*, 865 F.3d 1130, 1140 (9th Cir. 2017). It must also "draw all reasonable inferences in favor of the nonmoving party." *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987).

IV. DISCUSSION

Plaintiffs claim to represent five different potential classes of plaintiffs: the Worldwide Class,[2] the United States Sub-Class,[3] the California Sub-Class,[4] the CIPA Sub-Class,[5] and the

[2] "All natural persons whose personal information, or data derived from their personal information, was used to create a profile and made available for sale or use through Oracle's ID Graph or Data Marketplace."

[3] "All natural persons located in the United States whose personal information, or data derived from their personal information, was used to create a profile and made available for sale or use through Oracle's ID Graph or Data Marketplace."

[4] "All natural persons located in California whose personal information, or data derived from their personal information, was used to create a profile and made available for sale or use through Oracle's ID Graph or Data Marketplace."

[5] "All members of the California Sub-Class whose contents of their electronic communications were intercepted by the use of Oracle's bk-coretag.js functionality."

ECPA Sub-Class.[6] On behalf of these classes, the Complaint alleges seven causes of action: (1) Invasion of Privacy under the California Constitution (for the California Sub-Class); (2) Intrusion Upon Seclusion under California Common Law (on behalf of all classes); (3) Violation of the Unfair Competition Law under Cal. Bus. & Prof Code § 17200 *et seq.* (on behalf of all classes); (4) Violation of the California Invasion of Privacy Act (on behalf of the CIPA Sub-Class); (5) Violation of the Federal Wiretap Act, under 18 U.S.C. § 2510; (6) Unjust Enrichment (on behalf of all classes); and (7) Declaratory Judgment and Injunctive Relief (on behalf of all classes).

Defendant moves to dismiss all of the claims under 12(b)(1) and 12(b)(6). In addition to its substantive arguments, Defendant has also moved for certain paragraphs be stricken from the Complaint, and requests judicial notice of several documents.

A. Judicial Notice

Defendant requests judicial notice of twelve different documents, arguing Plaintiffs either refer to them extensively in the Complaint, or rely on them as a basis for their claims. Three of these are customer-facing company policies and agreements (Exhibit B: Oracle Advertising's Online Data Agreement; Exhibit H: AddThis Privacy Policy; and Exhibit J: Oracle Advertising Privacy Policy); the rest are Oracle web pages or press releases hosted on Oracle's own website.

There are two exceptions to the general rule that "district courts may not consider material outside the pleadings when assessing the sufficiency of a complaint under Rule 12(b)(6)": judicial notice and incorporation by reference. *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 998 (9th Cir. 2018). Courts may take judicial notice of matters that are either (1) generally known within the trial court's territorial jurisdiction or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. Fed. R. Evid. 201(b). As an alternative, the "incorporation by reference" doctrine is "a judicially created doctrine that treats certain documents as though they are part of the complaint itself," in order to "prevent[] plaintiffs

[6] "All members of the United States Sub-Class whose contents of their electronic communications were intercepted by the use of Oracle's bk-coretag.js functionality."

from selecting only portions of documents that support their claims, while omitting portions of those very documents that weaken—or doom—their claims." *Khoja*, 899 F.3d at 1002.

As Defendant correctly identifies, Plaintiffs make copious reference to Defendant's websites in the Complaint, and specifically hyperlink two of the requested documents (Exhibits J and H) in a footnote. At the same time, there is reason to "be cautious before taking judicial notice of documents . . . published on a website," "particularly . . . when a party seeks to introduce documents it created and posted on its own website," as is the case here. *Rollins v. Dignity Health*, 338 F. Supp. 3d 1025, 1033 (N.D. Cal. 2018). Likewise, the Ninth Circuit has warned that "incorporation by reference" is "improper" if used "to resolve factual disputes against the plaintiff's well-pled allegations in the complaint." *Khoja*, 899 F.3d at 1014 ("The incorporation-by-reference doctrine does not override the fundamental rule that courts must interpret the allegations and factual disputes in favor of the plaintiff at the pleading stage."). A document should not be incorporated if the defendant seeks its incorporation "merely [to] create[] a defense to the well-pled allegations in the complaint," as "[o]therwise, defendants could use the doctrine to insert their own version of events into the complaint to defeat otherwise cognizable claims." *Id.* at 1002.

Though Plaintiffs notably do not dispute the authenticity of the documents, judicially noticing all of the information contained on Oracle's own webpages is improper and unnecessary, as it would serve no purpose other than exactly what the Ninth Circuit warned against: crafting an alternative version of events. For the same reasons, Defendant's request to incorporate the documents by reference is denied, except as to Exhibits J and H, which are clearly referenced in Plaintiffs' allegations both by name and by link.[7]

[7] Although Exhibit B is generally referenced in the Complaint, *see, e.g.*, Dkt. 1 ¶ 38 ("Oracle has agreements with numerous high-traffic websites like the New York Times, ESPN, and Amazon to place cookies and/or pixels on their websites."), it is not used by Plaintiffs to the same degree as Exhibits J and H. As a result, it is inappropriate to find the document incorporated by reference.

B. Article III Standing (All Causes of Action)

Defendant first argues that the case must be dismissed, because Plaintiffs have failed to allege two of the three elements that make up the "irreducible constitutional minimum" of Article III standing under *Lujan*: (1) a concrete and particularized injury, that (2) is fairly traceable to Defendant's conduct. 504 U.S. at 560.

"'[A]n injury in fact' is 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Novak v. United States*, 795 F.3d 1012, 1018 (9th Cir. 2015) (quoting *Lujan*, 504 U.S. at 560) (alternation in original). Causation, the second element, requires a "causal connection between the injury and the conduct complained of." *Novak*, 795 F.3d at 1018 (9th Cir. 2015) (citing *Lujan*, 504 U.S. at 560). This element is concerned with ensuring that the injury is "fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court." *Lujan*, 504 U.S. at 560 (citing *Simon v. Eastern Ky. Welfare Rts. Org.*, 426 U.S. 26, 41–42 (1976)) (alternations in original).

While Plaintiffs' Complaint extensively quotes news articles and other outside sources painting a dramatic picture of Defendant's data brokerage business, it contains scarce specific allegations regarding the named Plaintiffs. In its claim that the Plaintiffs have not sufficiently pointed to a concrete and particularized harm, Defendant specifically argues that Plaintiffs have not alleged the profiles "were *actually* sold or made available for sale by Oracle to ***anyone***," Dkt. 23 at 6. Defendant further argues that any harm is not fairly traceable to Oracle, because Plaintiffs fail to allege that "Oracle tracked, profiled, or sold any of ***Plaintiffs***' personal information," Dkt. 23 at 8, and because there are "numerous third parties that made independent decisions leading to the alleged harm," which breaks the causal link. Dkt. 23 at 9.

Although the Complaint would indeed be much better served by the inclusion of more allegations specifically tying their general allegations of the "financial, dignitary, reputational, and relational harms [Defendant] has caused" to the named Plaintiffs, the Complaint is not so devoid of allegations that Plaintiffs' suit must be dismissed. Plaintiffs allege that Katz-Lacabe "received a

document from Oracle indicating Oracle had tracked, compiled, and analyzed his web browsing and other activity and thereby created an electronic profile on him," and that "Oracle continues to track [his] internet and offline activity, enrich the profile of him as described below, and make his personal information available to third parties without his consent." Dkt. 1 at 2. The Complaint provides similar but varied allegations for Plaintiffs Golbeck and Ryan, adding for the former that she "discovered Oracle tracking devices on multiple of her computers that she regularly uses for internet browsing and other activities," Dkt. 1 at 3, and asserting the allegations for Plaintiff Ryan on information and belief. As to all Plaintiffs, the Complaint's use of "as described below"—when construed in the light most favorable to them—references Defendant's data collection methods and attendant dangers generally described in the body of the Complaint, such as Oracle's ability to amass "vast amounts of personal data" for the purpose of "identify[ing] individuals and aggregat[ing] their many identifiers," Dkt. 1 at 7, the result of which is the creation of a "cradle-to-grave" profile[] of Class members." Dkt. 1 at 50. Such profiles are effectively dossiers which "can be used to further invade Plaintiffs' privacy" by "allowing third parties to learn intimate details of [Plaintiffs'] lives, and target them for advertising, political, and other purposes," ultimately "harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them." Dkt. 1 at 52. Altogether, these allegations are in line with those found in other cases in the Circuit and sufficiently allege harm to the Plaintiffs for Article III standing. *See, e.g*, *In re Facebook, Inc. Internet Tracking Litig.* ("*Facebook Tracking*"), 956 F.3d 589, 601 (9th Cir. 2020).

Defendant's other arguments about Plaintiffs' allegedly inadequate pleading of harm—including its attempts to distinguish relevant cases—are similarly unpersuasive. As the Ninth Circuit has recognized, invasion of privacy can be a harm in and of itself, *see Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017). Plaintiffs' case is not merely about a risk or inference of future harm. The letters that Plaintiffs received from Oracle indicate that Plaintiffs' data had been collected. The other inferences that Plaintiffs seek—including the harm that results from such data collection—are not altogether unreasonable, and must be accepted for the purposes

of the motion. Plaintiffs are not yet required to make specific allegations as to what particular information was purportedly sold. *See Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011) ("At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we 'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'") (quoting *Lujan*, 504 U.S at 561).

Defendant's argument that the string of causation is broken because of "numerous third parties" who made "independent decisions" misapprehends the law—a conclusion apparent from the cases to which it attempts to appeal. As the Ninth Circuit explains in *Maya*: "[t]o survive a motion to dismiss for lack of constitutional standing," plaintiffs are not required to show that the defendant's actions are the "'proximate cause' of plaintiffs' injuries"; instead, "plaintiffs must establish a 'line of causation' between defendants' action and their alleged harm that is more than 'attenuated.'" 658 F.3d at 1070 (citing *Allen v. Wright*, 468 U.S. 737, 757 (1984)). In fact, *Maya* counsels that "[a] causation chain does not fail simply because it has several 'links,' provided those links are 'not hypothetical or tenuous' and remain 'plausib[le].'" *Id.* (citations omitted). Here, Plaintiffs allege that Oracle's products, implemented by numerous websites, lead to the collection of vast amounts of data which, when "synchronized" altogether, lead to personal identification and purported invasions of privacy. That is, in fact, the very outcome that Oracle wishes—and markets to its customers. Plaintiffs' allegations simply do not hinge on hypothetical or tenuous links of causation the way that allegations of predatory lending to high-risk mortgagees necessarily result in decreased home values, *Maya*, 658 F. 3d at 1072, or that federal tax exemptions to racially discriminatory private schools impair school desegregation. *Wright*, 468 U.S. at 758-59 ("The chain of causation is even weaker in this case. It involves numerous third parties (officials of racially discriminatory schools receiving tax exemptions and the parents of children attending such schools) who may not even exist in respondents' communities and whose independent decisions may not collectively have a significant effect on the ability of public school students to receive a desegregated education."). Plaintiffs thus have alleged harm that fairly could be ascribed to Defendant, and they have Article III standing to maintain the present action.

C. First & Second Causes of Action: Invasion of Privacy (California Constitution) & Intrusion Upon Seclusion

The tests for an invasion of privacy under the California Constitution and intrusion upon seclusion under California common law "involve[] similar elements"—as a result, "courts consider the claims together" with one test, "and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Facebook Tracking*, 956 F.3d at 601 (citing *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)).

A reasonable expectation of privacy can exist where a defendant gains "unwanted access to data by electronic or other covert means, in violation of the law or social norms." *Facebook Tracking*, 956 F.3d at 601-02 (quoting *Hernandez*, 47 Cal 4th at 286). This determination entails a consideration of the customs, practices, and circumstances surrounding the data collection, such as "the amount of data collected, the sensitivity of data collected, the manner of data collection, and the defendant's representations to its customers." *Hammerling v. Google LLC*, No. 21-cv-09004-CRB, 2022 WL 2812188, at *10 (N.D. Cal. July 18, 2022) (citations omitted).

Evaluating whether Defendant's actions were "highly offensive" necessitates a "holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *Facebook Tracking*, 956 F.3d at 606 (quoting *Hernandez*, 47 Cal 4th at 287). This inquiry also "focuses on the degree to which the intrusion is unacceptable as a matter of public policy." *Id.*

Defendant invokes *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012) and cases cited therein to argue that California's constitution and common law "set a high bar for an invasion of privacy claim," *id.* at 1025, and to explain that even disclosure of social security numbers would not constitute an "egregious breach of social norms." *Id.* (citing cases). As the data allegedly collected was not sensitive in nature, and the company's data collection practices were publicly disclosed, Defendant argues, Plaintiffs could not have had a reasonable expectation of privacy, and Defendant's conduct was neither highly offensive nor egregious.

Plaintiffs' strongest argument lies in its allegation that Oracle's accumulation of a "vast repository of personal data," Dkt. 30 at 11—from compiling Plaintiffs' browsing activity, online communications, *and* offline activity—is what contravenes the reasonable expectation of privacy. This is in line with the analysis provided in *Facebook Tracking*. Explaining that technological advances, such as the "use of cookies to track and compile internet browsing histories," enable "access to a category of information otherwise unknowable and implicate privacy concerns," *Facebook Tracking*, 956 F.3d at 603, the Ninth Circuit found a reasonable expectation of privacy from "allegations that Facebook allegedly compiled highly personalized profiles from sensitive browsing histories and habits." *Id.* at 604; *see also Hammerling*, 2022 WL 2812188, at *11 (finding a reasonable expectation of privacy where Google collected a "large amount of personal information from users' smartphones").

Indeed, in differentiating *Facebook Tracking* from the analysis in *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) (where the Ninth Circuit expressed, in a footnote, that URLs might be constitutionally problematic due to the information it reveals about people's internet activity) and *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1108-09 (9th Cir. 2014) (where the Ninth Circuit declined to find a reasonable expectation of privacy in referral headers containing URLs), the Ninth Circuit explained that in *Facebook Tracking*, the search terms and URLs at issue "could divulge a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's platform." *Facebook Tracking*, 956 F.3d at 605.

Here, Plaintiffs allegations extend to "sensitive health and personal safety information," Dkt. 1 at 14-15, 27 ("Oracle's Health and Wellness segments reveal sensitive, health-related types of personal information Oracle collects on Class members."), and race and politics, *see* Dkt. 1 at 31-32, 44. While these are alleged generally and it is a close question as to whether Oracle plausibly did collect and aggregate information to reveal such insights, viewing the allegations in the light most favorable to Plaintiffs, such allegations of data collection would go well beyond the "routine commercial behavior" of collecting contact information for sending advertisements. Dkt. 23 at 17 (citing *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011)).

Finally, determinations of the egregiousness of the privacy intrusion are not usually

resolved at the pleading stage. *See Facebook Tracking*, 956 F.3d at 606 ("The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage."); *In re Facebook, Inc., Consumer Priv. User Profile Litig.* ("*Facebook Consumer Privacy*"), 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019) ("Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is."). Accordingly, Plaintiffs have alleged enough in the Complaint for these claims to withstand dismissal.

D. Third Cause of Action: UCL

The UCL provides a cause of action to challenge any "unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. While Plaintiffs allege that Defendant violated the first two (the unfair and unlawful prongs), both of these claims fail for lack of standing.

Over and above the demands of Article III, the UCL limits standing to those who have "suffered injury in fact and ha[ve] lost money or property as a result of . . . unfair competition." Cal. Bus. & Prof. Code § 17204. Thus, "[t]o satisfy the narrower standing requirements imposed by [§ 17204], a party must . . . (1) establish a loss or deprivation of money or property sufficient to qualify as injury in fact . . . and (2) show that the economic injury was the result of, i.e., *caused by*, the unfair business practice . . . that is the gravamen of the claim." *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 322 (2011) (emphasis in original).

Here, Plaintiffs fail to show they have an economic injury. Plaintiffs do identify some support for the idea that personal information without consent constitutes economic injury. *See Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) ("[T]he Ninth Circuit and a number of district courts, including this Court, have concluded that plaintiffs who suffered a loss of their personal information suffered economic injury and had standing.") (citing cases, including *In re Facebook Privacy Litig.* ("*Facebook Privacy*"), 572 F. App'x 494, 494 (9th Cir. 2014); and *In re Yahoo! Inc. Cust. Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017)). The weight of the authority in the district and the state, however, point in the opposite direction: that "the 'mere misappropriation of personal information' does not

establish compensable damages." *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App'x 613, 615 (9th Cir. 2021); *see also Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 540-41 & n.13 (2022) (noting that "[t]he scant California authority cited by *Facebook Privacy* did not address the value of PII, much less any deprivation thereof" and finding *Facebook Privacy* and district court cases following *Facebook Privacy* "unpersuasive."); *Facebook Consumer Privacy*, 402 F. Supp. 3d at 804 (distinguishing a company's gain of money through sharing or use of Plaintiffs' information from a claim that Plaintiffs actually lost money and dismissing Plaintiffs' theory of economic loss as "purely hypothetical"); *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1093 (N.D. Cal. 2018) ("However, the sharing of names, user IDs, location and other personal information does not constitute lost money or property for UCL standing purposes.") (citing *Campbell v. Facebook*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014); *Svenson v. Google Inc.*, 65 F. Supp. 3d 717, 730 (N.D. Cal. 2014) (finding that Plaintiff could not proceed with UCL claim because she had "not alleged any facts showing that Defendants' business practice—disclosing users' Contact Information to third-party App vendors—changed her economic position at all")). Because Plaintiffs have not alleged a specific monetary or economic loss, Plaintiffs lack standing to maintain their UCL claims.

E. Fourth and Fifth Causes of Action: CIPA & ECPA (Federal Wiretap Act)

Defendant raises three defenses to Plaintiffs' wiretapping claims: (1) Defendant is exempt from liability as a party to Plaintiffs' alleged communications; (2) Plaintiffs fail to plead the interception of "contents" as defined under the relevant statutes; and (3) Oracle's customers' consent satisfies one-party consent under the ECPA.

With respect to the first argument, Plaintiffs are correct that the weight of the authority in this Circuit teaches that Defendant is not a party to Plaintiffs' alleged communications. Defendant invokes *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021) to argue that it is simply "an extension" of the website operators, rather than an outsider. Yet such application ignores the analysis provided in *Noom* itself, which explains that the third-party "is a vendor that provides a software service that captures its clients' data, hosts it on [its own] servers, and allows the clients

to analyze their data." *Id.* at 832. Importantly, there were "no allegations . . . that [the vendor] intercepted and used the data itself," which rendered it altogether different from companies which "mined information from other websites and sold it." *Id.* In this analysis, *Noom* specifically distinguished *Facebook Tracking*—where "Facebook tracked its users to third-party websites (through Facebook's code on the websites) . . . and then it sold that data to advertisers," *Noom*, 533 F. Supp. 3d at 832—and *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019)—where "NaviStone was a marketing company that partnered with e-commerce sites to intercept visitor data and create marketing databases of consumer information." *Noom*, 533 F. Supp. 3d at 832. The situation at bar is far more analogous to those at issue in *Facebook Tracking* and *Revitch*[8]—and as such, Defendant is not a party to the communications.

With respect to Defendant's second argument, the definition of "contents" is similar under both the CIPA and the ECPA. *In re Google RTB Consumer Priv. Litig.*, 21-cv-2155-YGR, 2022 WL 2165489, at *11 (N.D. Cal. June 13, 2022) (citing *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020)). The Ninth Circuit has held that, under the ECPA, "'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *Zynga*, 750 F.3d at 1106. Of the nine types of information that Plaintiffs allege was captured by Defendant's bk-coretag.js code, then, only two are mainly at issue[9]: (1) referrer URLs; and (2) data entered into forms. Though Plaintiffs suggest that URLs "can also constitute contents of communications," Dkt. 30 at 18, Defendant argues that Plaintiffs fail to identify whether the URLs at issue here include elements that would render their collection problematic, such as search terms

[8] Defendant attempts to distinguish those cases, but as Plaintiffs have alleged that Oracle combines and sells information in its Data Marketplace, it appears that Defendant's products cannot be properly analogized to the tools in *Noom*.

[9] Defendant is correct that the other seven pieces of information, which include webpage titles, webpage keywords, the date and times of website visits, IP addresses, page visits, purchase intent signals, and add-to-cart actions, are conceded to be record information that does not constitute "content" under the ECPA. *See Zynga*, 750 F.3d at 1106 ("[R]ecord information . . . includes the 'name,' 'address,' and 'subscriber number or identity' of a subscriber or customer.").

which would reveal the content a user searched for, *see Zynga*, 750 F.3d at 1108, or full-string detailed URLs that might contain folder and file names. *Facebook Tracking*, 956 F.3d at 605. While Plaintiffs' lack of specificity makes this a close call, the allegation about the data entered into forms resolves the question in their favor. Though Defendant correctly notes the absence of a blanket rule that all entries in a web form are content, its suggestion that *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003) only found disclosure of contents because Plaintiffs entered personal medical information into a web form reads the decision too narrowly. Instead, the First Circuit explained that the definition of contents "encompasses personally identifiable information such as a party's name, date of birth, and medical condition." *Id.* at 18. For both of these pieces of information, when the allegations are construed in the light most favorable to Plaintiffs, they have pled *just barely enough* to withstand dismissal at this juncture.

Finally, Defendant is correct that the federal Wiretap Act is a one-party consent statute, pursuant to 18 U.S.C. § 2511(2)(d). As Defendant's customers must have chosen to deploy Oracle's tools on their websites, it necessarily follows that "one of the parties to the communication"—the websites themselves—gave "prior consent to such interception." *Id; see also Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1026 (N.D. Cal. 2014) ("[T]he consent of one party is a complete defense to a Wiretap Act claim."). Plaintiffs' attempt to invoke the crime-tort exception, requiring them to plead sufficient facts to show that "the primary motivation or a determining factor in the interceptor's actions has been to injure plaintiffs tortiously," does not apply to a case such as this, where Defendant's "purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money." *Rodriguez*, 2021 WL 2026726 at *6 n.8 (citing *In re Google Inc. Gmail Litigation*, No. 13-MD-02430-LHK, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014). As a result, Plaintiffs' Wiretap Act claim must be dismissed on this basis while their CIPA claim survives.

F. Sixth Cause of Action: Unjust Enrichment

Defendant next seeks to dismiss Plaintiffs' unjust enrichment claim, explaining that no

such standalone cause of action exists in California law and that Plaintiffs have failed to allege mistake, fraud or coercion, or that a benefit was conferred on Oracle that would be unjust for it to retain.

Though "in California, there is not a standalone cause of action for 'unjust enrichment,'" *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015), "[w]hen a plaintiff alleges unjust enrichment, a court may 'construe the cause of action as a quasi-contract claim seeking restitution.'" *Id.* (quoting *Rutherford Holdings, LLC v. Plaza Del Rey*, 223 Cal. App. 4th 221, 231 (2014)). "To allege unjust enrichment as an independent cause of action, a plaintiff must show that the defendant received and unjustly retained a benefit at the plaintiff's expense." *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016).[10]

Plaintiffs do not demonstrate that Defendant has unjustly retained a benefit at Plaintiffs' expense. While they argue "a right to disgorgement of profits resulting from unjust enrichment," Plaintiffs' appeal to *Facebook Tracking* misses the opinion's full context: "California law requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable." *Facebook Tracking*, 956 F.3d at 600. Here, Plaintiffs and putative class members have neither directly expended their own resources, nor shown that their property has become less valuable. Unlike the Plaintiffs in *Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592 (N.D. Cal. 2021), Plaintiffs here were at no time in direct privity with Oracle. As a result, Defendant did not collect information from Plaintiffs in a manner contrary to expectations created by the consent process. *See id.* at 597 (noting users'

[10] Plaintiffs are mistaken that *Astiana*, which continues to be applied in this Circuit, is no longer good law. *See, e.g., Hillori Graham v. Central Garden & Pet Co.*, No. 22-CV-06507-JSC, 2023 WL 2744391, at *3 n.2 (N.D. Cal. Mar. 30, 2023); *Day v. Advanced Micro Devices, Inc.*, No. 22-CV-04305-VC, 2023 WL 2347421, at *1 n.1 (N.D. Cal. Mar. 2, 2023). Moreover, "[t]he argument that California law does not recognize a cause of action for unjust enrichment is for all intents and purposes a nonstarter," as "California law recognizes, at a minimum, a quasi-contract claim based on an unjust-enrichment theory." Day, 2023 WL 2347421 at *1 n.1 (citing both *Astiana*, 783 F.3d at 762 and *ESG Cap. Partners*, 828 F.3d at 1038). Litigants' appeal to semantics is therefore resisted, and the unjust enrichment claim will be construed in accordance with the direction from the Ninth Circuit, as conveyed in *Astiana* and *ESG Capital Partners*.

information was tracked even when the application was not open, and that "[n]owhere in the consent process was the user confronted with the information that their minute-by-minute geolocation data [would] be broadly disseminated by [Defendant] and that [Defendant] would make millions disseminating users' geolocation data").[11] Without more, Plaintiffs have not stated a claim for unjust enrichment.

G. Choice of Law

Defendant takes issue with Plaintiffs' assertion of California state claims on behalf of non-California residents—both named Plaintiffs Golbeck and Ryan (residents of Florida and Ireland, respectively), as well as the classes that include non-residents (e.g., the nationwide and worldwide classes)—and seek dismissal of those claims on this basis. As this order dismisses the UCL, ECPA and unjust enrichment claims, the only remaining claim at issue is Plaintiffs' intrusion upon seclusion claim alleged under California common law.

Both parties are in agreement that "[a] federal court sitting in diversity must look to the forum state's choice of law rules," thus requiring the court to apply California's "governmental interest approach" to determine questions of choice of law. *Zinser v. Accufix Rsch. Inst., Inc.*, 253 F.3d 1180, 1187 (9th Cir. 2001). This is a three-step process. The first task is to determine whether the laws of the affected jurisdictions are "the same or different." *Mazza v. American Honda Motor Co., Inc.*, 666 F.3d 581, 590 (9th Cir. 2012) (quoting *McCann v. Foster Wheeler LLC*, 48 Cal. 4th 68, 81-82 (2010)). If the laws are different, the second step requires an examination of "each jurisdiction's interest in the application of its own law" to determine whether a true conflict exists. *Id.* If it does, then the final step involves analyzing "which state's interest would be more impaired if its policy were subordinated to the policy of the other state." *Id.*

Applying this analysis, Defendant explains that significant differences exist between California's law that of Florida and the GDPR that render it inappropriate to apply California law

[11] To the extent Defendant has data, moreover, it was received and/or collected with permission from the third-party websites. If Plaintiffs challenge unjust enrichment based on the monetization of that data, they must explain why the access they received to those websites would not defeat the unjust enrichment claim.

to the latter two. In response, Plaintiffs contend that Defendant's choice of law analysis is too sparse to fulfill its burden of displacing California law, and, in the alternative, that such analysis is premature at the pleadings stage.

Plaintiffs are correct that district courts in this Circuit have often deferred choice-of-law issues until the class certification stage. *See, e.g., Wallace v. SharkNinja Operating, LLC*, No. 18-cv-05221-BLF, 2020 WL 1139649, at *15 (N.D. Cal. Mar. 9, 2020). However, "whether a choice-of-law analysis can be properly conducted at the motion to dismiss stage depends on the individual case." *Bartel v. Tokyo Elec. Power Co., Inc.*, 371 F. Supp. 3d 769, 790 (S.D. Cal. 2019). "To determine whether the choice-of-law analysis should occur on the pleadings or at class certification, courts generally look to whether discovery would be a meaningful aid to that inquiry." *Anderson v. Apple Inc.*, 500 F. Supp. 3d 993, 1010 (N.D. Cal. 2020) (collecting cases). When it is unlikely that further fact development would materially impact the choice of law determination, that determination need not be deferred. *Frenzel v. AliphCom*, 76 F. Supp. 3d 999, 1007–08 (N.D. Cal. 2014) (dismissing individual and class claims at the motion to dismiss stage where named plaintiff was "a nonresident who did not purchase the defendant's product in California").

That is the case here. With respect to Florida, Defendant notes it specifically requires a plaintiff to show an intrusion into a private quarter. *Hammer v. Sorensen*, 824 F. App'x 689, 695 (11th Cir. 2020) (plaintiffs are required "to show an intrusion into a private place and not merely a private activity") (citing *Allstate Ins. Co. v. Ginsberg*, 863 So. 2d 156, 161 n.3, 162 (Fla. 2003)).

Plaintiffs insist Defendant's analysis is not "rigorous," in that it only identifies "superficial differences in . . . language," which are minimal, as both Florida and California rely on the Restatement of Torts (Second) to define intrusion upon seclusion. Dkt. 30 at 8. These general arguments are not themselves an answer, however, to the differences that Defendant has raised. The requirement of a private quarter is an element of the claim in Florida that is not an explicit requirement in California. As California requires a plaintiff to show only that there exists a reasonable expectation of privacy, and that whatever intrusion on plaintiff's privacy was "highly

offensive," *Facebook Tracking*, 956 F.3d at 601, which in turn necessitates consideration of legal and social norms and circumstances surrounding the data collection and intrusion, there is indeed a possibility that a successful claim under California law would fail to be meritorious under the law of Florida. Indeed, such a conclusion, particularly for cases like the one at bar, is bolstered by Defendant's explanation that "Florida's laws have not stretched to reach" claims premised on the collection of online data, Dkt. 35 at 5, as well as Florida's failure to enact consumer privacy legislation conferring substantive data privacy rights in the way that California has done. *See* Dkt. 35 at 5 n.8 (comparing H.B. 9, 2022 Fla. Leg., Reg. Sess. (Fla. 2022) (unenacted) and S.B. 1864, 2022 Fla. Leg., Reg. Sess. (Fla 2022) (unenacted) with Cal. Civ. Code §§ 1798.100, *et seq.*). Moreover, even though Florida relies on the Restatement, the Eleventh Circuit has noted, specifically with respect to the private quarter requirement, that "the Supreme Court of Florida has construed the tort of intrusion upon seclusion even more narrowly than the Restatement provides." *Hammer*, 824 F. App'x at 695 (citing *Allstate*, 863 So. 2d at 161 n.3, 162).

Because this difference is neither "trivial [n]or wholly immaterial," each state's interest in applying its law must be analyzed. *Mazza*, 666 F.3d at 591. California recognizes that "with respect to regulating or affecting conduct within its borders, the place of the wrong has the predominant interest," *id.* at 593 (citing *Hernandez v. Burger*, 102 Cal. App. 3d 795, 802 (1980)), where the "place of the wrong" is defined as "the state where the last event necessary to make the actor liable occurred." *Id.* (citing *McCann*, 48 Cal. 4th at 94 n.12 (geographic location of an omission is the place of the transaction where it should have been disclosed) and *Zinn v. Ex–Cell–O Corp.*, 148 Cal. App. 2d 56, 80 n.6 (1957) (concluding in a fraud case that the place of the wrong was the state where the misrepresentations were communicated to the plaintiffs, not the state where the intention to misrepresent was formed or where the misrepresented acts took place)). Additionally, "California's interest in applying its law to residents of foreign states is attenuated," *id.* at 594 (citing *Edgar v. MITE Corp.*, 457 U.S. 624, 644 (1982)), particularly where "the claims of foreign residents concern[] acts that took place in other states." *Id.*

Here, although Oracle is headquartered in California,[12] Plaintiffs interactions with the third-party websites do not necessarily take place in California—and presumably do not, when considering Plaintiffs Golbeck and Ryan. Therefore, even if some of the challenged conduct allegedly emanated from California, it is not enough to establish California's interest, particularly where the "last event[s]" involved in the collection and interception of data (e.g., the third-party websites' decision to use Oracle's services) were made possible by an intermediary that may or may not be located in the state. *See Mazza*, 666 F.3d at 594 ("[T]he last events necessary for liability as to the foreign class members—communication of the advertisements to the claimants and their reliance thereon in purchasing vehicles—took place in the various foreign states, not in California. These foreign states have a strong interest in the application of their laws to transactions between their citizens and corporations doing business within their state.") Reliant on tests requiring courts to assess whether expectations about privacy are reasonable or data collection is egregious, privacy is an evolving area of law that is inherently tied to community standards. In light of this and the apparent differences in the legal framework among states, Plaintiffs have failed to show that the law of California should be applied nationwide.

The even greater legal differences between intrusion upon seclusion under California's laws and the GDPR leads to a similar conclusion for Plaintiffs' Worldwide class. Defendant raises several differences that would impact the present matter, including that the GDPR: lacks an "evaluation of contemporary social norms," Dkt. 23 at 10, provides a "comprehensive policy framework" that clearly describes the legal requirements, Dkt. 35 at 6,[13] and requires

---

[12] During the hearing, Defendant raised the factual issue that Oracle moved its headquarters out of California. Although this choice of law analysis proceeds on the assumption that Oracle was headquartered in California, it is noted that this issue would be relevant for determining class definitions (such as timelines), and would only present additional hurdles in the choice of law analysis for selecting California as the law to apply nationally and globally.

[13] *Compare, e.g., Facebook Tracking*, 956 F.3d at 601 (describing the tests for an invasion of privacy under both the California Constitution and intrusion upon seclusion as an inquiry of two elements—"whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive"), *with*, GDPR Art. 4(11) ("'[C]onsent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.") *and id.* Art. 6(1)(a) ("Processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent to the

intermediaries for consumers to bring class actions (*i.e.*, consumers cannot do so directly). Because such legal differences are significant and Plaintiffs have not explained what evidence additional discovery could adduce, the choice of law analysis can be made at this juncture. Accordingly, the intrusion upon seclusion claim (applying California common law) for Plaintiffs' nationwide and global classes cannot stand.

H. Seventh Cause of Action: Declaratory Judgment

Plaintiffs' declaratory judgment claim will rise and fall with its other claims: if Plaintiffs fail to allege facts sufficient to state a claim under any other cause of action, the claim for declaratory judgment will be dismissed. As not all of Plaintiffs' claims have been dismissed, the declaratory judgment claim survives to that extent.

I. Equitable Relief

Defendant cites *Sonner v. Premier Nutrition Corp.* for the proposition that a plaintiff cannot seek equitable relief "for past harm under the UCL and CLRA" unless she first "establish that she lacks an adequate remedy at law." 971 F.3d 834, 844 (9th Cir. 2020). Under *Sonner*, Defendant argues, Plaintiffs' equitable claims should be dismissed, because Plaintiffs have not shown they lack an adequate remedy at law. Plaintiffs respond that *Sonner* does not apply to their request for prospective injunctive relief, nor does it bar remedies that "go beyond" damages, Dkt. 30 at 24, or equitable relief asserted in the alternative.

"[T]he import of Sonner at the pleading stage is an unsettled question of law and has given rise to an intra-circuit split." *Yeomans v. World Fin. Grp. Ins. Agency, Inc.*, No. 19-cv-00792-EMC, 2022 WL 844152, at *7 (N.D. Cal. Mar. 22, 2022) (collecting cases). Plaintiffs are correct that "*Sonner* does not preclude a plaintiff from pleading equitable remedies in the alternative." *Id.* at *8. Notably, some courts have found that "*Sonner* has limited applicability to the pleading stage because it pertained to circumstances in which a plaintiff dropped all damages claims on the eve of trial," *Jeong v. Nexo Fin. LLC*, No. 21-cv-02392-BLF, 2022 WL 174236, at *27 (N.D. Cal. Jan. 19, 2022), circumstances which do not even remotely exist here. *See Yeomans*, 2022 WL 844152,

---

processing of his or her personal data for one or more specific purposes. . . .").

at *7 ("*Sonner* teaches that a plaintiff, on the eve of trial, cannot create an inadequacy of a legal remedy by eliminating its availability by taking volitional action."). Because the cases are distinguishable, and because "[t]he issue of Plaintiff's entitlement to seek the equitable remedy of restitution may be revisited at a later stage," *Nacarino v. Chobani, LLC*, No. 20-cv-07437-EMC, 2022 WL 344966, at *10 (N.D. Cal. Feb. 4, 2022), Defendant's motion to dismiss the claims for equitable relief is denied.

J. Motion to Strike

Federal Rule of Civil Procedure 12(f) permits a court to strike "any redundant, immaterial, impertinent, or scandalous matter" from a pleading. The purpose of a motion to strike is primarily "to avoid the expenditure of time and money that must arise from litigating spurious issues by dispensing with those issues prior to trial." *Whittlestone, Inc. v. Handi-Craft Co.*, 618 F.3d 970, 973 (9th Cir. 2010) (quotation omitted).

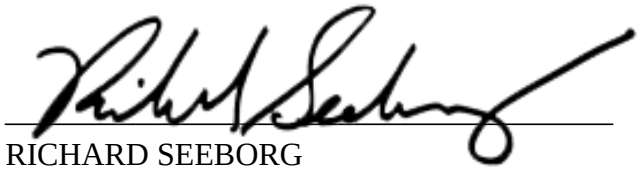
Defendant's request to strike the allegations in Paragraphs 64-65, 76-81, and 147 as redundant and immaterial is not well taken. Motions to strike are "generally disfavored," *XpertUniverse, Inc. v. Cisco Sys., Inc.*, No. 17-cv-03848-RS, 2019 WL 3413309, at *3 (N.D. Cal. July 29, 2019) (citations omitted). The paragraphs in question concern topics related to Plaintiffs' allegations about Defendant—including, broadly, data brokers and data potentially available on Defendant's Data Marketplace. Contrary to Defendant's argument, none of the information contained therein presents content so prejudicial or immaterial and irrelevant as to warrant their removal at this juncture. Accordingly, Defendant's request to strike is denied.

V. CONCLUSION

In light of the above, Plaintiffs' UCL, ECPA, unjust enrichment, and intrusion upon seclusion (on behalf of the Worldwide and United States sub-classes) claims are dismissed without prejudice, whereas their remaining claims—invasion of privacy, intrusion upon seclusion (for the California sub-class), CIPA, declaratory judgment and equitable relief—survive, albeit some barely. Defendant's motion to strike is denied, and its request for incorporation by reference is granted only as to Exhibits J and H. Plaintiffs are given 30 days to file an amended complaint.

IT IS SO ORDERED.

Dated: April 6, 2023



RICHARD SEEBORG
Chief United States District Judge

United States District Court
Northern District of California