2023 WL 7392285
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

Amin JAMES, et al., Plaintiffs,
v.
The WALT DISNEY COMPANY, Defendants.

Case No. 23-cv-02500-EMC (EMC)
|
Signed November 8, 2023

Synopsis

Background: Visitors to sports media website filed putative class action lawsuit against website's owner, alleging that their privacy rights, as protected by Pennsylvania and California statutory law, have been violated because there was third-party software embedded in website that captured and collected data as individuals used the website. Owner moved to dismiss for lack of standing and for failure to state a claim.

Holdings: The District Court, Edward M. Chen, J., held that:

visitors had facial standing to assert class action claims against website's owner for alleged violations of their privacy rights;

visitors plausibly alleged that owner intended that software intercept their personal information for its own use;

visitors did not plausibly allege that owner intended software intercept their personal information for use by third-party's other customers;

visitors plausibly alleged that owner intercepted contents of their communications;

software could constitute device under Pennsylvania Wiretapping and Electronic Surveillance Control Act (WESCA);

visitors plausibly alleged that software intercepted their personal information while it was in transit; and

material differences between California Invasion of Privacy Act (CIPA) and wiretapping statutes of other states precluded nationwide application of California law to visitors' putative class action claims.

Motion granted in part and denied in part.

Procedural Posture(s): Motion to Dismiss for Lack of Standing; Motion to Dismiss for Failure to State a Claim.

Attorneys and Law Firms

L. Timothy Fisher, Bursor & Fisher, P.A., Walnut Creek, CA, Max Stuart Roberts, Pro Hac Vice, Bursor & Fisher P.A., New York, NY, for Plaintiffs.

Vassiliki Iliadis, Hogan Lovells U.S. LLP, San Francisco, CA, Allison M. Holt-Ryan, Pro Hac Vice, Hogan Lovells U.S. LLP, Washington, DC, James W. Ettinger, Hogan Lovells U.S. LLP, Los Angeles, CA, for Defendants.

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS

Docket No. 15

EDWARD M. CHEN, United States District Judge

***1** Plaintiffs Amin James and David Sevesind (collectively, "Plaintiffs") have filed a class action against Defendant The Walt Disney Company ("Disney"). Plaintiffs assert that their privacy rights, as protected by Pennsylvania and California statutory law, have been violated because there is Oracle software embedded in Disney's ESPN.com website that captures and collects data as individuals use the website (*e.g.*, pages viewed, keystrokes, mouse clicks, etc.). Currently pending before the Court is Disney's motion to dismiss for lack of standing and for failure to state a claim for relief.

Having considered the parties' briefs as well as the oral argument of counsel, the Court hereby **GRANTS** in part and **DENIES** in part Disney's motion.

I. FACTUAL & PROCEDURAL BACKGROUND

In their complaint, Plaintiffs allege as follows.

Disney is a company that owns and operates the website ESPN.com. *See* Compl. ¶ 8. Embedded on the ESPN.com website is Oracle software, in particular, a tool known as Oracle BlueKai which is part of a line of products known as Oracle CX. [1] BlueKai intercepts and collects website visitors' electronic communications with the website. *See* Compl. ¶¶ 1, 14, 17. The data collected is used to market to and attract new customers for Disney. *See* Compl. ¶ 22. Furthermore, "Oracle does not simply manage their clients' data[;] Oracle also retains and uses the same data to assist *other* clients" (*i.e.*, clients other than Disney). Compl. ¶ 30 (emphasis added).

> 23. To enable Oracle to track website users, website owners insert a "Core Tag" – "bk-coretage.js" – into their webpages and applications, unbeknownst to the webpage or application visitor.
>
> 24. When a user visits a website that has Core Tag in the code, the user's browser sends a "GET request" to the website server. The server responds by sending HTML code to the user's browser. The HTML code includes a JavaScript that contains the Core Tag which instructs the user's browser to send another GET request to Oracle. Oracle then utilizes the Core Tag to collect data for BlueKai. Through this process, Oracle is able to extract the website visitor user attributes.
>
> ....
>
> 26. The data Oracle BlueKai collects includes but is not limited to:
>
> (a) HTML page properties;
>
> (b) Pages viewed;
>
> (c) Purchase intent;
>
> (d) Add-to-cart actions;
>
> (e) Keystrokes;
>
> (f) Search terms entered; and
>
> (g) "Mouse click events."
>
> ....
>
> 31. To summarize, website owners a Core Tag onto their websites, which enables Oracle BlueKai to collect significant user data. Oracle then associates that data to a specific user, compiles that data with other data about the user Oracle has in its possession, and provides that data to website owners to enable website owners to hyper target users in marketing campaigns. Oracle then retains that data and uses it to assist other website owners.

Compl. ¶¶ 23-24, 26, 31 (footnotes omitted).

[1] Oracle CX is short for "Oracle Advertising and Customer Experience." *See* Compl. ¶ 14. "Oracle CX is used to '[b]uild a complete view of your customer and their every Interaction – no matter how, when, where, or with whom they engage.' " Compl. ¶ 15.

***2** According to Plaintiffs, Disney entered into a "contractual arrangement" with Oracle "to intercept communications between [Disney] and visitors to the [ESPN.com] website." Compl. ¶ 33.

Mr. James is a resident of Pennsylvania and, in December 2022, visited the ESPN.com website on his computer. *See* Compl. ¶ 5. Mr. Davis is a resident of California and, in May 2023, visited the website on his computer. *See* Compl. ¶ 6. When each used the website, his communications on the website were intercepted by Oracle. *See* Compl. ¶¶ 37-38; *see also* Compl. ¶ 5 (referring to keystrokes, mouse clicks, and "other communications").

Based on, *inter alia*, the above allegations, Plaintiffs have asserted two causes of action: (1) a violation of the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. C.S. § 5701 *et seq.*; and (2) a violation of the California Invasion of Privacy Act. *See* Cal. Pen. Code § 631. Plaintiffs have identified three different classes: (1) a nationwide class of all persons who visited the ESPN.com website and who had electronic communications intercepted; (2) a Pennsylvania subclass; and (3) a California subclass. *See* Compl. ¶¶ 40-42.

Although not entirely clear, it appears that Plaintiffs are suing Disney because Oracle intercepted data for the benefit of Disney *and* because Oracle then used that data for the benefit of other companies as well.

II. DISCUSSION

A. Legal Standard

As noted above, Disney seeks to dismiss both for lack of standing and failure to state a claim for relief. The motion to dismiss for lack of standing is brought pursuant to Federal

Rule of Civil Procedure 12(b)(1), and for failure to state a claim for relief pursuant to Rule 12(b)(6).

A Rule 12(b)(1) motion for lack of standing can be facial in nature or factual. *See Pride v. Correa*, 719 F.3d 1130, 1139 (9th Cir. 2013). "In a facial attack, the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction. By contrast, in a factual attack, the challenger disputes the truth of the allegations that, by themselves, would otherwise invoke federal jurisdiction." *Safe Air For Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). Here, Disney makes a facial attack on standing.

To overcome a Rule 12(b)(6) motion to dismiss after the Supreme Court's decisions in *Ashcroft v. Iqbal*, 556 U.S. 662, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009), and *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007), a plaintiff's "factual allegations [in the complaint] 'must ... suggest that the claim has at least a plausible chance of success.' " *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014). The court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). But "allegations in a complaint ... may not simply recite the elements of a cause of action [and] must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Levitt*, 765 F.3d at 1135 (internal quotation marks omitted). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678, 129 S.Ct. 1937. "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (internal quotation marks omitted).

B. Rule 12(b)(1) Motion – Standing

***3** Disney argues first the Court lacks subject matter jurisdiction over the case because, based on the allegations in the complaint, Plaintiffs do not have standing. Disney's argument is based on a Supreme Court decision, *TransUnion LLC v. Ramirez*, —— U.S. ——, 141 S. Ct. 2190, 210 L.Ed.2d 568 (2021), and several district court cases that have interpreted *TransUnion.*

TransUnion involved a class action where claims for violation of the Fair Credit Reporting Act ("FCRA") were asserted. According to the named plaintiff, TransUnion violated the FCRA based on a product it offered called OFAC Name Screen Alert.

> OFAC is the U. S. Treasury Department's Office of Foreign Assets Control. OFAC maintains a list of "specially designated nationals" who threaten America's national security. Individuals on the OFAC list are terrorists, drug traffickers, or other serious criminals. It is generally unlawful to transact business with any person on the list. TransUnion created the OFAC Name Screen Alert to help businesses avoid transacting with individuals on OFAC's list.

Id. at 2201. The product, however, "generated many false positives" because it would place an alert on a credit report indicating a potential match based on first and last names only. *Id.* The plaintiff alleged that TransUnion violated the FCRA when, *e.g.*, it failed to follow reasonable procedures to ensure the accuracy of information in his credit file. *See id.* at 2202.

Before trial, the parties stipulated that (1) the class had 8,185 members but that (2) "only 1,853 members ... had their credit reports disseminated by TransUnion to potential creditors" during the relevant period. *Id.* The district court held that *all* 8,185 members had Article III standing. *See id.* The issue before the Supreme Court was whether that decision on standing was correct.

The focus of the Supreme Court was whether the class members had suffered an injury in fact – *i.e.*, a concrete injury that was real and not abstract. *See id.* at 2203. The Supreme Court asked:

> What makes a harm concrete for purposes of Article III? As a general matter, the Court has explained that "history and tradition offer a meaningful guide to the types of cases that Article III empowers federal courts to consider." And with respect to the concrete-harm requirement in particular, this Court's opinion in *Spokeo v. Robins* indicated that courts should assess whether the alleged injury to the plaintiff has a "close relationship" to a harm "traditionally" recognized as providing a basis for a lawsuit in American courts.

> That inquiry asks whether plaintiffs have identified a close historical or common-law analogue for their asserted injury. *Spokeo* does not require an exact duplicate in American history and tradition. But *Spokeo* is not an open-ended invitation for federal courts to loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts.
>
> As *Spokeo* explained, certain harms readily qualify as concrete injuries under Article III. The most obvious are traditional tangible harms, such as physical harms and monetary harms. If a defendant has caused physical or monetary injury to the plaintiff, the plaintiff has suffered a concrete injury in fact under Article III.
>
> Various intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion.

***4** *Id.* at 2204. Critically, in *Transunion* as in *Spokeo*, the asserted harm was reputational in nature, a harm akin to defamation.

The Supreme Court then noted that "Congress's views may be 'instructive' " in "determining whether a harm is sufficiently concrete to qualify as an injury in fact." *Id.* But it emphasized that, "even though 'Congress may "elevate" harms that "exist" in the real world before Congress recognized them to actionable legal status, it may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is.' " *Id.* at 2205. A plaintiff does not satisfy the injury-in-fact requirement just because " 'a statute grants a person a statutory right and purports to authorize that person to sue to indicate that right.' " *Id.* (also stating that "Congress's creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III"). It was in this context that the Supreme Court stated: " 'Article III standing requires a concrete injury even in the context of a statutory violation,' " and, "under Article III, an injury in law is not an injury in fact." *Id.*

Turning to the facts of the case before it, the Supreme Court assumed that TransUnion did in fact violate its obligations under the FCRA to use reasonable procedures in internally maintaining credit files. The question for the Court was whether *all* 8,185 class members suffered a concrete harm as a result of the company's failure to use reasonable procedures. *See id.* at 2208.

The Supreme Court held that the "1,853 class members ... whose reports were [actually] disseminated to third-party businesses" did suffer a concrete harm. *Id.* The injury to these class members bore "a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts – namely, the reputational harm associated with the tort of defamation." *Id.* Notably, the Court stated that,

> [i]n looking to whether a plaintiff's asserted harm has a "close relationship" to a harm traditionally recognized as providing a basis for a lawsuit in American courts, we do not require an exact duplicate. The harm from being labeled a "potential terrorist" bears a close relationship to the harm from being labeled a "terrorist."

Id. at 2209.

However, the remaining 6,332 class members did not suffer a concrete harm given the absence of dissemination of their credit information to any potential creditors. The Court explained that this was because "[p]ublication is 'essential to liability' in a suit for defamation .... [T]here is 'no historical or common-law analog where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury.' " *Id.*; *see also id.* at 2210 n.6 (stating that "plaintiffs' internal publication theory circumvents a fundamental requirement of an ordinary defamation claim – publication – and does not bear a sufficiently 'close relationship' to the traditional defamation tort to qualify for Article III standing").

***5** Disney argues that, under *TransUnion*, Plaintiffs are asserting an intangible harm which amounts to invasion of privacy. Disney then asserts that Plaintiffs' claims do not have a sufficiently close relationship to a claim for invasion of privacy because such a claim requires that a plaintiff's *personal* information be at issue and, here, Plaintiffs have not alleged that their personal information was intercepted by Oracle. *See* Mot. at 9 ("Plaintiffs do not allege that their

person or otherwise private information was intercepted by Oracle. Rather, Plaintiffs claim that a narrow set of non-sensitive *record* information was collected ....") (emphasis in original). Disney adds that, even if some sensitive interactions were intercepted, that would not be " 'highly offensive' to a reasonable internet user.' " Mot. at 10. Disney maintains that Plaintiffs would have to show that interception of the information was highly offensive because "[t]he closest equivalent common law claim is that of intrusion upon seclusion," and such a claim requires that the intrusion be highly offensive to a reasonable person. *See* Mot. at 9.

As an initial matter, the Court rejects Disney's argument that Plaintiffs must show that any interception of information was highly offensive in order to have standing. Disney assumes that the closest analogue is a claim for intrusion upon seclusion. However, the Ninth Circuit's decision in *In re Facebook Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020), establishes that there are other kinds of privacy rights fairly at issue here. In *Facebook*, the plaintiffs filed suit based on Facebook's practice of using plug-ins to track users' browsing histories when they visited third-party websites. *See id.* at 596. The Ninth Circuit held that the plaintiffs had standing to assert, *e.g.*, their privacy-based claims (both statutory and common law) because the "right to privacy 'encompass[es] the individual's control of information concerning his or her person.' " Id. at 598. That is the privacy right being claimed by Plaintiffs here. To the extent Disney suggests that *Facebook* is no longer good law after *TransUnion*, the Court disagrees. Nothing about *TransUnion* guts the above holding in *Facebook*, particularly because *Facebook* postdates *Spokeo*, the precedent on which *TransUnion* largely relied. Furthermore, the Ninth Circuit has not disavowed *Facebook* in the wake of *TransUnion*. *See, e.g., Jones v. Ford Motor Co.*, No. 22-35447, 2023 U.S. App. LEXIS 28600 at *6 (9th Cir. Oct. 27, 2023). (citing *Facebook* approvingly).

As for Disney's other contention, the Court agrees that a privacy claim is dependent on personal information being implicated (similar to a defamation claim requiring that there be a publication or dissemination of information). But contrary to what Disney claims, Plaintiffs have sufficiently asserted personal information. Plaintiffs have alleged, for instance, that information intercepted by Oracle included information about, *e.g.*, specific web pages viewed, search terms entered, and purchase behavior. *See, e.g.*, Compl. ¶¶ 5, 6, 26, 36.[2] In addition, Plaintiffs have alleged that the information that is collected is not anonymized. *See* Compl. ¶¶ 27-28 (alleging, *inter alia*, that the Oracle software "creates and sends a 'unique user ID' ").

2 The Court acknowledges that the complaint does not expressly tie the allegations made in ¶¶ 26 and 36 to Plaintiffs specifically. However, all reasonable inferences are to be made in Plaintiffs' favor at this juncture of the proceedings. Here, it can reasonably be inferred that the list of information that BlueKai collects applies to Plaintiffs.

Again, *Facebook* is instructive. In *Facebook*, the Ninth Circuit held that Plaintiffs had established standing because they had

> alleged harm to [their] privacy interests. Plaintiffs alleged that Facebook continued to collect their data after they had logged off the social media platform, in order to receive and compile their personally identifiable browsing history. As alleged in the complaint, this tracking occurred "no matter how sensitive" or personal users' browsing histories were. Facebook allegedly constantly compiled and updated its database with its users' browsing activities, including what they did when they were not using Facebook. According to Plaintiffs, by correlating users' browsing history with users' personal Facebook profiles – profiles that could include a user's employment history and political and religious affiliations – Facebook gained a cradle-to-grave profile without users' consent.
>
> ***6** Here, Plaintiffs have adequately alleged that Facebook's tracking and collection practices would cause harm or a material risk of harm to their interest in controlling their personal information. As alleged, Facebook's tracking practices allow it to amass a great degree of personalized information. Facebook's user profiles would allegedly reveal an individual's likes, dislikes, interests, and habits over a significant amount of time, without affording users a meaningful opportunity to control or prevent the unauthorized exploration of their private lives.

Id. at 598-99.

To be sure, *Facebook* seems to have involved more personal information than what was allegedly intercepted in the instant case. Even so, intercepting information about, *e.g.*, pages viewed, search terms entered, or purchase behavior (as alleged here) is sufficiently similar in nature to intercepting

information about, *e.g.*, a person's likes or dislikes (as in *Facebook*). Moreover, as indicated above, Plaintiffs have alleged that the collection of information is not anonymized. At the very least, Plaintiffs have made sufficient allegations to create a question of fact as to whether there is sufficiently personal information to support standing. This is especially true given that, *Facebook* aside, there is other authority (albeit some of it dated pre-*TransUnion*) that supports Plaintiffs' position that the information at issue is sufficiently personal. *See, e.g.*:

- *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3d Cir. 2019) (stating that "[h]istory and tradition reinforce that a concrete injury for Article III standing purposes occurs when Google, or any other third party, tracks a person's *internet browser activity* without authorization") (emphasis added).

- *Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC 2019 U.S. Dist. LEXIS 186955, at *1-3 (N.D. Cal. Oct. 23, 2019) (concluding that plaintiff had standing with respect to his claim that defendant helped another company "eavesdrop on his communications" made on defendant's website; communications included plaintiff requesting information from defendant "by *clicking on items of interest*") (emphasis added).

- *Carter v. Scripps Networks, LLC*, No. 22-cv-2031 (PKC), 2023 U.S. Dist. LEXIS 71150 at *3, 8 (S.D.N.Y. Apr. 24, 2023) (denying motion to dismiss for lack of standing where plaintiffs alleged that HGTV transmitted to Facebook information that allowed Facebook to identify which videos each plaintiff had viewed on hgtv.com; "defendants' alleged disclosure of plaintiffs' *personal information and viewing activities* describes traditionally recognized harm") (emphasis added).

The lower court cases cited by Disney are largely distinguishable. For example, in *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034 (N.D. Cal. 2022) (Gonzalez Rogers, J.), was a data breach case. That context clearly informed the district court's assessment – in conducting a standing analysis under *TransUnion* – that "it is not clear ... how the discovery of a password to a gaming account would be 'highly offensive to a reasonable person,' particularly where there is no allegation that the gaming accounts for which plain text passwords were taken contain confidential information." *Id.* at 1049.

In *Massie v. General Motors LLC*, No. 21-787-RGA, 2022 U.S. Dist. LEXIS 28969, at *12 (D. Del. Feb. 17, 2022), the plaintiffs challenged the defendant's use of certain software on its website that recorded, *e.g.*, website users' mouse movements, clicks, and keystrokes. *See id.* at *4. The plaintiffs browsed the vehicle sections of the website but did not make any purchases and did not input any personal information such as name, zip code, phone number, and email address. *See id.* The district court held that the plaintiffs did not have standing but this appears to have been predicated in part on the fact that the data captured was anonymized. *See id.* at *12 ("Plaintiffs do not have a reasonable expectation of privacy over the anonymized data captured by the Session Replay software at issue here."); *id.* at *3 ("I agree that Plaintiffs have a legally cognizable interest in controlling their personal information [but] none of Plaintiffs' personal information is implicated by the allegations they make. Plaintiffs fail to explain how either GM's or Decibel's possession of anonymized, non-personal data regarding their browsing activities on GM's website harms their privacy interests in any way."). As noted above, Plaintiffs have made allegations indicating that the information collected was not anonymized.

***7** In *Lightoller v. JetBlue Airways Corp.*, No. 23-cv-00361-H-KSC, 2023 WL 3963823, 2023 U.S. Dist. LEXIS 102158 (S.D. Cal. June 12, 2023), the plaintiff also challenged software that "enables website operators to record, save, and replay a website visitor's interactions with a given website, including 'mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of webpages visited, and/or other electronic communications in real-time.' " *Id.* at *2. The district court found a lack of standing explaining as follows:

> Although Plaintiff alleges that Defendant monitored and recorded her communications via software when she visited Defendant's website, Plaintiff does not allege that she disclosed any personal information when she visited the website. As such, no personal information was intercepted and recorded. The only internet communications specifically alleged in the complaint is that Plaintiff "obtain[ed] information on flight pricing." Flight pricing information is not personal information.

Id. at *10. Here, Plaintiffs have made allegations that the information collected was more than just mere pricing information. To the extent *Lightoller* is read to hold non-anonymized information on, *e.g.*, websites visited or search terms used is not sufficiently personal, the Court disagrees.

There is, however, one argument that Disney makes that has some merit. That is, even though, as discussed above, some of the information that Oracle allegedly collected seems sufficiently personal, Plaintiffs have been somewhat vague and conclusory about other information that was allegedly intercepted. *Cf. Straubmuller v. JetBlue Airways Corp.*, No. DKC 23-384, 2023 WL 5671615 at *4, 2023 U.S. Dist. LEXIS 155704 at *9 (D. Md. Sept. 1, 2023) ("Because the Complaint says nothing about the kinds of interactions Plaintiff had with Defendant's website, much less the specific kinds of captured personal information implicating a substantive privacy interest, Plaintiff has not alleged that his personal information was intercepted and recorded by Defendant.").

For example:

- Mr. James: "During the [website] visit, Mr. James's keystrokes, mouse clicks, and other communications – such as the specific web pages he viewed – were intercepted in real time by Oracle. Mr. James was unaware at the time that his keystrokes, mouse clicks, and other electronic communications were being intercepted in real-time by Oracle, nor did Mr. James consent to the same." FAC ¶ 5.

- Mr. Sevesind: "During the [website] visit, Mr. Sevesind's keystrokes, mouse clicks, and other communications – such as the specific web pages he viewed – were intercepted in real time by Oracle. Mr. Sevesind was unaware at the time that his keystrokes, mouse clicks, and other electronic communications were being intercepted in real-time by Oracle, nor did Mr. Sevesind consent to the same." FAC ¶ 6.

Plaintiffs have sufficiently overcome the 12(b)(1) challenge to the extent they have referred to webpages viewed, searches conducted, purchase behavior, and so forth. That is enough to support standing. But simply referring to keystrokes, mouse clicks, and "other communications" – without additional allegations – would standing alone arguably be insufficient. Of course, any insufficiency would not detract from the standing that has been established. However, because the Court is, as discussed below, granting in part Disney's 12(b)(6) motion with leave to amend, it would behoove Plaintiffs to include in their amended complaint more specific allegations about the keystrokes, mouse clicks, and "other communications."

C. Rule 12(b)(6) Motion – Claim for Relief

***8** Because the Court concludes that Plaintiffs have adequately alleged standing, it must address Disney's 12(b)(6) motion for failure to state a claim for relief. Disney raises several challenges to the two statutory claims asserted by Plaintiffs. Some of the arguments apply to both the Pennsylvania claim and the California claim; other arguments are specific to either the Pennsylvania claim or the California claim.

The Pennsylvania Wiretapping and Electronic Surveillance Control Act (WESCA) provides in relevant part that "[a]ny person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a); *see also id.* § 5703(1) (providing that it is a crime if a person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication"). In their complaint, Plaintiffs emphasize the "procure[ ]" element. *See* Compl. ¶ 51 ("To establish liability under [WESCA], Plaintiffs need only to establish that Defendant 'procure[d] any other person to intercept [electronic] communication.' ").

The California Invasion of Privacy Act (CIPA) provides in relevant part:

> [a]ny person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and

> without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable ....

Cal. Pen. Code § 631(a). In their complaint, Plaintiffs emphasize the "aids, agrees with, employs, or conspires" element. [3] *See* Compl. ¶ 66 ("At all relevant times, Defendant aided, agreed with, employed, conspired with, or otherwise enabled Oracle to wiretap consumers to the Website using Chat [sic] and to accomplish the wrongful conduct at issue here.").

3 At the hearing, Plaintiffs admitted that, if Disney had collected the information *itself* (*i.e.*, not using Oracle or any other third party to do the collection), then there would be no WESCA or CIPA violation. This is because Disney was a party to the communications at issue (*i.e.*, a recipient of the communications made by the website users), and thus it could not have "intercepted" any communications. Plaintiffs maintain that, even though Disney hired Oracle to do the collection *for* Disney, that does not protect Disney from liability. In the pending motion, Disney makes no argument that it cannot be held liable because all that Disney did was hire a third party to engage in conduct that Disney could have lawfully done itself.

1. Intent

***9** In the pending motion to dismiss, Disney makes somewhat of an elaborate argument with respect to Plaintiffs' "procure"/"aid" theory (*e.g.*, invoking the rule of lenity because the statutes are criminal, referencing different statutes on aiding and abetting, etc.). However, as reflected in Disney's reply brief, that argument boils down to a relatively simple one: namely, that (1) Disney cannot be held liable under WESCA or CIPA unless it *intended* to have Oracle intercept the information at issue and that (2) Plaintiffs have failed to plead such an intent. *See, e.g.*, Reply at 6 (arguing that, in order for a claim to be viable, Plaintiffs must plead "Disney's knowledge of the purported wiretap or its intent" because, otherwise, the statutes would be strict liability statutes "which is contrary to the text of these criminal statutes"); Reply at 6 (adding that, for direct-party liability, the defendant must have willfully or intentionally intercepted the information at issue, so "[t]he Court should not endorse a lesser form of *mens rea* for third-party liability than for direct-party liability under the same statute"); Reply at 7. According to Disney, "far from possessing the specific intent to aid Oracle in the unlawful interception of Plaintiffs' communications without Plaintiffs' consent, Disney affirmatively disclosed that their website contained tracking technologies, including technologies such as BlueKai, and empowered users to set their own tracking preferences." Mot. at 15 n.9.

Plaintiffs do not fundamentally dispute that there must have been intent on the part of Disney to have Oracle intercept. Their position is that they have sufficiently pled intent in the complaint – *i.e.*, one can infer Disney intended to have Oracle intercept because Disney entered into a contract with Oracle so that Oracle would provide such services. *See* Compl. ¶ 17 ("Oracle CX offers a marketing tool ('Oracle BlueKai' or 'BlueKai') through which Oracle can collect data on Oracle's clients' customers in order to market and attract new customers."); Compl. ¶ 33 ("Defendant enabled, allowed, or otherwise procured Oracle to intercept communications between Defendant and visitors to the ESPN website through a contractual website."). Plaintiffs maintain: "This is common sense ... as Oracle could not place its BlueKai software on Defendant's website without Defendant's permission." Opp'n at 7; *see also* Opp'n at 9 ("[G]iven Oracle's BlueKai software did not appear on Defendant's website out of nowhere, and that Defendant benefits greatly from Oracle's services, it is clear Defendant 'intended' for Oracle to eavesdrop on website visitors.").

Plaintiffs have the stronger position. As they maintain, it can reasonably be inferred that Disney entered into a contractual arrangement with Oracle under which Oracle would collect

information from EPSN.com website users *so that Disney could market to and attract new customers*. Disney may have an argument that website users agreed to tracking when they used the website, but that is a question of fact that cannot be determined at the 12(b)(6) phase of the proceedings.

There is, however, one problem with Plaintiffs' position with respect to the issue of intent. Specifically, to the extent Plaintiffs seek to hold Disney liable because Oracle used the information it collected for its clients *other* than Disney, then they must make allegations that Disney knew Oracle would use the information collected for the benefit of other Oracle customers. In other words, while it can reasonably be inferred that Disney knew Oracle would intercept for the benefit of Disney, it cannot reasonably be inferred that Disney knew Oracle would intercept for the benefit of a company other than Disney.

Accordingly, the Court dismisses Plaintiffs' statutory claims to the extent they seek to hold Disney liable for Oracle intercepting and then using the information at issue for non-Disney clients. Plaintiffs have leave to amend, if they can do so in good faith.

2. Contents of Communication

According to Disney, even if Plaintiffs adequately alleged intent, they have still failed to state a claim for relief because they have not sufficiently alleged that any "contents" of a communication were intercepted. This argument applies to both the WESCA claim and the CIPA claim.

WESCA provides in relevant part that "[a]ny person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a). "Intercept" is defined as "[a]ural or other acquisition of the *contents* of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." *Id.* § 5702 (emphasis added).

***10** CIPA provides in relevant part that

> [a]ny person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection ... with any telegraph or telephone wire, line, cable, or instrument ..., or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the *contents* or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable ....

Cal. Pen. Code § 631(a) (emphasis added).

According to Disney, in the case at bar, Plaintiffs have not adequately alleged *what* the contents of any intercepted communications are; instead, Plaintiffs have only vaguely referred to, *e.g.*, webpages viewed, mouse clicks, and keystrokes. *See* Mot. at 16 ("Plaintiffs do not allege what specific Website webpages they visited, or what information they purportedly provided to Disney in the course of their visit. Such conclusory allegations do not suffice.").

Disney further contends that, to the extent Plaintiffs have identified categories of information that were intercepted, that kind of information does not constitute the contents of a communication but rather is at most "record information." Disney cites in support, *inter alia, Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110 (N.D. Cal. 2020). There, the district court noted that (1) " '[t]he analysis for a violation of CIPA is the same as that under the federal Wiretap Act' "; that (2) the Wiretap Act defines "contents" as " 'any information concerning the substance, purport, or meaning of that communication' "[4]; and that (3) per the Ninth Circuit, " 'record information regarding the characteristics of the message that is generated in the course of the

communication' does not qualify as 'contents.' " *Id.* at 127; *see also Cook v. GameStop, Inc.*, No. 2:22-cv-1292, 2023 U.S. Dist. LEXIS 150953 at *17 (W.D. Penn. Aug. 28, 2023) (in discussing Pennsylvania's Wiretap Act, stating that "determining whether a plaintiff has adequately pled a violation of the statute often comes down to deciding whether the acquired information can best be characterized as either 'record information' or 'the message conveyed by the communication' "). [5]

[4] *See also In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (discussing the meaning of "contents" under federal law; "Congress intended the word 'contents' to mean a person's intended message to another (i.e., the 'essential part' of the communication, the 'meaning conveyed,' and the 'thing one intends to convey')").

[5] In *Zynga Privacy Litigation*, the Ninth Circuit noted that, under federal law, "record information includes, among other things, the 'name,' 'address,' and 'subscriber number or identity' of 'a subscriber to or customer of such service.' " *Zynga Privacy Litig.*, 750 F.3d at 1104. However, the Ninth Circuit also agreed with the proposition that record information "can become content if the record is the subject of a communication." *Id.* at 1107 (taking note of a First Circuit case where "the users had communicated with the website by entering their personal medical information into a form provided by a website"; under these circumstances, "the First Circuit correctly concluded that the defendant was disclosing the contents of a communication").

***11** For the most part, Disney's arguments lack merit. For example, to the extent Disney suggests Plaintiffs must plead the exact communications they had with the ESPN.com website, other courts have rejected that position. *See, e.g., Byars v. Tire*, No. 5:22-cv-01358-SSS-KKx, 2023 U.S. Dist. LEXIS 22337, at *11-12 (C.D. Cal. Feb. 3, 2023) (stating that "[t]here is no requirement that [plaintiff] specifically allege the exact contents of her communications with Goodyear"; "[plaintiff] merely needs to show that the contents were not record information such as her name and address").

To the extent Disney asserts Plaintiffs must have more specificity in their complaint to show that record information is not at issue, Plaintiffs have met that threshold – at least in part. Plaintiffs have alleged that Oracle intercepted, *e.g.*, information about the webpages they viewed and searches they conducted. This makes it unlikely that Plaintiffs are simply implicating record information – *i.e.*, information regarding the characteristics of a message as opposed to the substance of the message itself. *Cf. Zynga Privacy Litig.*, 750 F.3d at 1108-09 (acknowledging that, "[u]nder some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication").

To be sure, to the extent Plaintiffs claim that the "contents" of communications that were intercepted were mouse clicks and keystrokes without any further specification, there is arguably a closer call. *Compare Cook*, 2023 U.S. Dist. LEXIS 150953, at *21-22 (in discussing Pennsylvania's Wiretap Act, stating that mouse clicks do not "plausibly reveal the substance of any communication"; such conduct is "the kind of 'routing information' that has historically not been recognized as content" or, alternatively, is just a "record of ... movements within a digital space" and "[a]ny 'substance' that can flow from these movements must be inferred from the observer, and therefore are not communicative"), *with Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 518 (C.D. Cal. 2021) (stating that "[n]ot all of this information may constitute the 'contents' of a communication under the federal Wiretap Act, [but] Plaintiff has met his burden to allege facts plausibly showing Defendants recorded Plaintiff's content communications with Nike by recording, among other things, keystrokes and a video of Plaintiff's interactions with Nike's website"). While the prior discussion identifies cases which hold that information such as pages viewed, search terms, purchases made, etc. may be sufficiently private to implicate cognizable privacy interests, the Court need not definitively decide whether the rather conclusory allegations about mouse clicks and keystrokes are sufficient since it is already giving Plaintiffs an opportunity to plead more specific facts with respect to mouse clicks and keystrokes (as discussed above in conjunction with the Rule 12(b)(1) motion).

3. Device (WESCA Claim Only)

Disney's arguments above on intent and contents have applied to both the WESCA and CIPA claims. However, Disney has also offered some arguments that are specific to each statutory claim. With respect to the WESCA claim, Disney argues that Plaintiffs have failed to state a claim for relief because they have failed to plead that a "device" was used to intercept communications.

***12** As noted above, WESCA provides in relevant part that "[a]ny person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a). "Intercept" is defined as "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other *device*." Id. § 5702 (emphasis added). "Electronic, mechanical or other device" in turn is defined as "[a]ny device or apparatus, including, but not limited to, an induction coil or a telecommunication identification interception device, that can be used to intercept a wire, electronic, or oral communication other than [certain exceptions not applicable here]." *Id.*

According to Disney, Plaintiffs have failed to plead the use of a device in the instant case because the term "device" means a physical or tangible object and not something intangible such as software. Disney's position is not entirely without merit, but the Court rejects it.

As an initial matter, the Court takes note that only one court – a federal district court in Pennsylvania – has expressly addressed the issue of whether "device" as used in WESCA includes software. The decision is *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108 (W.D. Pa. 2019) (hereinafter *Popa I*). In *Popa I*, the plaintiff alleged that the defendants unlawfully collected her data while she was shopping online. HCG was the company that owned the website; Navistone was the company that allegedly collected her data on HCG's website. The defendants argued that "HCG's servers and Navistone's [software] code are not 'devices,' and therefore their conduct does not fall within the sweep of WESCA." *Id.* at 116. The court did not outright reject the defendants' position, but it made a ruling that favored the plaintiff (at least for the time being), holding that the issue "warrant[ed] deeper factual exploration than was available at the motion to dismiss stage." *Id.*

In reaching this conclusion, the court noted that WESCA broadly defined the term "device."

> The use of the word "any" before the phrase "device or apparatus" in Section 5702 implies that the class of technology contemplated by WESCA is broad. So too for the kinds of "electronic communications" that are within WESCA's purview.
>
> ....
>
> While the statutory definitions of "device" and "electronic communication" are broad, they are not limitless. They may or may not include the type of electronic data collection complained of by Popa. To prevail on a claim under WESCA, it is Popa's burden to prove that the allegedly actionable conduct falls under the purview of the statute. The nature of the conduct involved makes it less than clear at this stage. Indeed, whether the interplay between Defendants' servers and Navistone's code qualifies as a "device" or "apparatus" is a fact intensive inquiry that implicates novel questions. The discovery process will give the parties an opportunity to develop a record that contextualizes the conduct at issue in light of this statutory language.

Id. at 117 (emphasis added). [6]

6 Both parties have also cited *Commonwealth v. Smith*, 136 A.3d 170 (Pa. Super. Ct. 2016), in support of their respective positions. However, *Smith*, unlike *Popa I*, did not squarely address the issue of whether software can be deemed a "device" under WESCA. The issue in *Smith* was whether a smartphone – which had been used to record a conversation by using a "voice memo" application – constituted a device for purposes of WESCA. *See id.* at 173. The trial court held that a smartphone was not a device based on an exemption under the statute for telephones and any components thereof. *See id.* The appellate court held that

> the trial court's interpretation of the Act leads to an absurd result. Disregarding the fact that the smartphone technology at issue was not available at the time the relevant subsection was enacted, Smith improperly, electronically, recorded his private conversation with Mojdeh, without Mojdeh's consent. The fact that Smith used an app on his smartphone, rather than a tape recorder, to do so, if of no moment.

Id. at 174. The appellate court stated at one point in its decision that "the 'device' at issue herein was a cellphone," but, at another point, it stated that "the trial court erred when it determined that Smith's use of a 'voice memo' app on his smartphone did not constitute an interception 'device.' " *Id.* at 178. Ultimately, the court was not called upon to

> expressly address the issue of whether software can be a device – or whether software in conjunction with whatever runs the software can be a device.

***13** In light of *Popa I*, the Court rejects Disney's position here that software – whether by itself or in conjunction with something else – can never be a device under WESCA. Moreover, Disney's position is problematic because it ignores the fundamental fact that, in order for software to work, it must be run on some kind of computing device. It is artificial to claim that software must be viewed in isolation from the computing device on which it runs and with which it is inseparable in regard to the challenged conduct.

Disney's arguments to the contrary are unavailing. For example, to the extent Disney has relied on dictionary definitions for "device," its position is problematic for several reasons. First, under Pennsylvania law, statutory construction begins with the plain language of the statute.

> We will only look beyond the plain language of the statute when words are unclear or ambiguous, or the plain meaning would lead to "a result that is absurd, impossible of execution or unreasonable." Therefore, when ascertaining the meaning of a statute, if the language is clear, we give the words their plain and ordinary meaning.

Ruhlman v. Ruhlman, 291 A.3d 916, 921 (Pa. Super. Ct. 2023). It is far from clear that the plain and ordinary meaning of "device" is limited to a physical or tangible object. *Cf. Kohl v. New Sewickley Twp. Zoning Hearing Bd.*, 108 A.3d 961, 969 (2015) (stating that a court "may draw upon common sense and basic human experience to construe terms").

Second, even though "[d]ictionaries should be used as source material to identify a word's 'common and approved usage,' " *Franks v. State Farm Mut. Auto. Ins. Co.*, 263 A.3d 1169, 1172 (Pa. Super. Ct. 2021); *see also Commonwealth v. Gamby*, 283 A.3d 298, 307 (Pa. 2022) (stating that, "[t]o discern the legislative meaning of words and phrases, our Court has on numerous occasions engaged in an examination of dictionary definitions"; indicating that the definition at the time of enactment is relevant, as is whether the definition remained consistent over time), Disney has not provided *actual copies* of the dictionary definitions (*e.g.*, as part of a request for judicial notice) but rather has selectively quoted from some dictionary definitions in its brief. *See* Mot. at 18-19. This is especially troubling because, at the very least, Disney seems to have mischaracterized a dictionary definition from Black's Law Dictionary. Disney asserts that the eleventh edition (2019) defines "device" as " '[a] mechanical invention' or 'an apparatus or an article of manufacture' and cross-referenc[es] 'machine.' " Mot. at 18. But it appears that Black's gave this definition in the context of *patents*. The definition of "device" in the eighth edition (2004) of Black's is as follows: "1. *Patents.* A mechanical invention, as differentiated in patent law from a chemical discovery. A device may be an apparatus or an article of manufacture. – Also termed *machine.* 2. A scheme to trick or deceive; a stratagem or artifice, as in the law relating to fraud." Black's Law Dictionary (8th ed. 2004). Notably, this definition also underscores that a device need not be a physical or tangible thing, but rather can be intangible, because the term is also used in, *e.g.*, the context of fraud.

Disney argues still that some courts have held that a "device" does not include software when considering statutes similar to WESCA – *i.e.*, addressing wiretapping and electronic surveillance. But notably, *this* Court has indicated that software can be a "device" for purposes of the federal Wiretap Act. *See In re Carrier IQ*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015) (stating in a header that "Plaintiffs Have Adequately Alleged that the Carrier IQ Software is a 'Device' for Purposes of the Wiretap Act"; also stating in text that the plaintiffs' operative complaint "properly alleges that the Carrier IQ Software is an '[e]lectronic, mechanical, or other device' which 'can be used to intercept a wire, oral, or electronic communication' "); *see also Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125-26 (3d Cir. 2022) (hereinafter *Popa II*) (stating that "[WESCA] operates in conjunction with and as a supplement to the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*, which provides uniform minimum protections for wire, electronic, or oral communications"). Admittedly, the focus in *Carrier IQ* was on one of the exceptions to "device"; specifically, there was an exception for a telephone or any component thereof being used by a provider of wire or electronic communication service in the ordinary course of its business. However, because the Court essentially found that there were questions of fact as to whether the exception applied, *see id.* (stating that "whether the Carrier IQ Software, as alleged, was used by the mobile carriers in their 'ordinary course of business' cannot be resolved at this stage"), that meant it concluded software *could* be a "device" under the federal Wiretap Act. *See also United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) (stating that "[t]he majority of courts to consider [the] issue have entertained the notion that software may be considered a device for purposes of the [federal] Wiretap Act"; citing cases). [7]

7 In an earlier decision issued in *Hutchins*, the district court pointed out that

> there are reasons to doubt such a strict interpretation of the Wiretap Act would be warranted .... Determining that the Wiretap Act could never apply to software would require the court to overlook the notably broad language of the Wiretap Act, which was to generally prohibit unauthorized artificial interception of communication in an era of changing technologies, in favor of a hyper-technical reading of the statute. It would also require the court to adopt a very restrictive definition of "electronic, mechanical, or other device" that may not comport with legislative intent, the ordinary meaning of those words, or the (scant) existing case law.

United States v. Hutchins, No. 17-CR-124, 2018 U.S. Dist. LEXIS 183898 at *36-37 (E.D. Wis. Oct. 26, 2018).

***14** To be sure, Disney is correct in noting that some courts have held software cannot be a "device" for purposes of non-Pennsylvania statutes on wiretapping/electronic surveillance. Disney has pointed to, in particular, several decisions addressing Florida's wiretap statute (known as the Security of Communications Act). *See, e.g., Jacome v. Spirit Airlines Inc.*, No. 2021-000947-CA-01, 2021 Fla. Cir. LEXIS 1435, at *14 (June 17, 2021) (holding that plaintiff failed to allege that the software at issue was a "device" under the Florida statute; taking note that "other courts have held that software, email servers, and drives [do] not constitute devices under the wiretapping statutes"). But *Jacome*'s citation to decisions concerning servers and drives is not particularly persuasive given that those decisions were predicated on the fact that the servers or drives simply *received* the information at issue, *i.e.*, there was no interception. *See, e.g., Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (Orrick, J.) ("Amazon did not ... 'intercept' the communication within the meaning of the Wiretap Act, because Amazon did not acquire it using a device other than the drive or server on which the e-mail was received. The fact that this necessarily entailed storage of the communication is not relevant. As the Ninth Circuit has noted, some storage is essential to communication via e-mail. Amazon merely received the information transferred to it by Crowley, an act without which there would be no transfer. Amazon acted as no more than the second party to a communication. This is not an interception as defined by the Wiretap Act."). This leaves Disney with the argument that the rule of lenity should weigh in its favor. *See Commonwealth v. Booth*, 564 Pa. 228, 766 A.2d 843, 846 (Pa. 2001) ("[W]here ambiguity exists in the language of a penal statute, such language should be interpreted in the light most favorable to the accused."). Assuming the rule of lenity applies to this civil action because the predicate statute imposes criminal liability, this argument is not particularly compelling for reasons similar to those articulated by the *Hutchins* court (albeit when addressing the federal Wiretap Act) – *i.e.*, WESCA uses broad language and engaging in a "hyper-technical reading of the statute" is inconsistent with what is presumably the purpose of the statute, *i.e.*, to "prohibit unauthorized artificial interception of communication in an era of changing technologies." *Hutchins*, 2018 U.S. Dist. LEXIS 183898, at *36-37; *see also Commonwealth v. Spangler*, 570 Pa. 226, 232, 809 A.2d 234 (2002) (stating that WESCA "emphasizes the protection of privacy").

4. In Transit (CIPA Claim Only)

Disney next launches a challenges to the CIPA claim. Disney asserts that the relevant portion of CIPA requires that any interception take place while a communication is "in transit," *i.e.*, before it reaches the intended recipient. *See* Cal. Pen. Code § 631(a) (providing that "[a]ny person ... who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is *in transit* or passing over any wire, line, or cable, or is being sent from, or received at any place within this state ... is punishable") (emphasis added); *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1137 (E.D. Cal. 2021) (stating that "the crucial question ... is whether Mastel has plausibly alleged that Miniclip read one of his communications while it was still in transit, i.e., before it reached its intended recipient"). Plaintiffs agree on this legal point. Where the parties disagree is whether Plaintiffs' complaint actually alleges that the interceptions by Oracle took place while communications were in transit between Plaintiffs and the ESPN.com website.

Below are the relevant passages from the complaint:

> 19. Oracle describes Oracle BlueKai DMP [data management platform] "as a large data warehouse where you can store, organize, and analyze all the customer data you've collected .... You can gather data directly by adding simple snippets of code called 'tags' to your web pages. The DMP will then track the user's journey."

....

23. To enable Oracle to track website users, website owners insert a "Core Tag" ... into their webpages and applications, unbeknownst to the webpage or application visitor.

24. When a user visits a website that has CoreTag in the code, the user's browser sends a 'GET request' to the website server. The server responds by sending HTML code to the user's browser. The HTML code contains a JavaScript that contains the Core Tag which instructs the user's browser to send another GET request to Oracle. Oracle then utilizes the Core Tag to collect data for BlueKai. Through this process, Oracle is able to extract the website visitor user attributes....

***15** 25. Oracle intercepts this user data in real-time (*i.e.*, simultaneously with a user's interaction with a website).

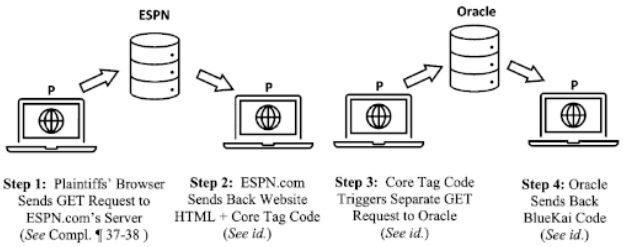
....

37. Plaintiff James and other Class Members accessed the ESPN website through their internet browsers in Pennsylvania. Upon having their browsers access the website in Pennsylvania, the browser sent a GET request from Pennsylvania to the ESPN website's servers. The ESPN website then sent a signal to web browser instructing the browser in Pennsylvania to send another GET request to Oracle. The web browser then sent another GET request from Pennsylvania to Oracle, which then began tracking Plaintiff James and Class Member's communications on ESPN.

38. Plaintiff Sevesind and other Class Members accessed the ESPN website through their internet browsers in California. Upon having their browsers access the website in California, the browser sent a GET request from California to the ESPN website's servers. The ESPN website then sent a signal to web browser instructing the browser in California to send another GET request to Oracle. The web browser then sent another GET request from California to Oracle, which then began tracking Plaintiff Sevesind and Class Member's communications on ESPN.

Compl. ¶¶ 19, 23-25, 37-38.

Disney takes the position that Plaintiffs have failed to meet the in-transit requirement by focusing on ¶ 24 above and largely ignoring the other paragraphs. According to Disney, ¶ 24 establishes that "BlueKai does not intercept any purported communications between Plaintiffs and the Website while the communications are 'in transit.' Rather, the Core Tag triggers a *second, distinct and sequential* data transmission between Plaintiffs' web browsers and Oracle." Mot. at 21 (emphasis in original).



Mot. at 22.

The problem for Disney is that the process above simply seems to lay out how BlueKai code gets to a website user's device. Disney ignores the paragraphs surrounding ¶ 24 which indicate that, once BlueKai is on the device, it *then* begins to intercept communications *when the user makes communications to the website. See, e.g.*, Compl. ¶ 25 ("Oracle intercepts this user data *in real-time (i.e., simultaneously with a user's interaction with a website)*.") (emphasis added); Compl. ¶ 37 ("The web browser then sent another GET request from Pennsylvania to Oracle, which *then* began tracking Plaintiff James and Class Member's communications on ESPN.") (emphasis added). [8]

[8] In their brief, Plaintiffs argue that, "[e]ven if the communications rested temporarily on Defendant's servers before being passed to Oracle – and 'resting' is a loose term given the speed of these communications – such 'resting' was 'transient,' 'intrinsic to the communications process,' and occurred 'contemporaneous[ly] with their transmission.' " Opp'n at 18; *cf. In re Carrier IQ*, 78 F. Supp. 3d at 1080 (agreeing with the First Circuit that "a communication in 'transient electronic storage that is intrinsic to the communication process for such communications' was not a stored communication for purposes of the [federal] ECPA").

***16** Notably, Disney's opening brief recognizes this possible reading of Plaintiffs' complaint. In its brief, Disney maintains that the complaint does *not* suggest the process outlined in ¶ 24 "only occurs once initially, then the BlueKai sits on the user's browser simultaneously collecting any further website

interactions. Rather, this process is repeated *each time* the user engages a webpage element that includes the Core Tag code." Mot. at 22 (emphasis added). But Disney's contention that the process in ¶ 24 is repeated "each time" is based solely on the fact that ¶ 24 states: "Through this process, Oracle is able to extract the website user attributes." Compl. ¶ 24. While arguably that statement could be read as Disney contends, it may also reasonably be understood to mean that this is the process that *starts* Oracle's ability to track with BlueKai. And at 12(b)(6), all reasonable inferences are to be made in Plaintiffs' favor, not Disney's.

5. Nationwide Class for CIPA Claim

The final issue for the Court concerns Plaintiffs' allegation that, because Disney "is headquartered in California, a CIPA [claim] can be pursued by all users of the Website nationwide." Compl. ¶ 68. In other words, Plaintiffs maintain that there can be a nationwide class based on CIPA alone, rather than the privacy laws of the various states. (Plaintiffs also assert a California subclass for the CIPA claim – effectively, as a backup.) Disney argues that, if Plaintiffs are asserting a CIPA claim, then the class cannot be nationwide in scope but rather should be limited to California plaintiffs – *i.e.*, because any alleged interception took place where the website user resided.

In response, Plaintiffs first make a procedural argument. Specifically, they argue that Disney's argument is tantamount to a motion to strike and not a motion to dismiss. Plaintiffs also assert that Disney's argument is premature and should wait until the class certification stage.

Plaintiffs' contention that Disney should have brought a motion to strike and not a motion to dismiss does not have much practical significance. The more important question is whether Disney should be allowed to make its challenge now or whether the challenge should be deferred until class certification. *Cf. Vallejo v. Sterigenics U.S., LLC*, No. 3:20-cv-01788-AJB-AHG, 2021 U.S. Dist. LEXIS 191072, at *6 (S.D. Cal. Oct. 4, 2021) (stating that "several courts within this Circuit have held that Rule 12(b)(6) is an improper vehicle for dismissing class claims and should rather be addressed through Rule 23[;] [m]oreover, while class allegations can be stricken at the pleadings stage if the claim could not possibly proceed on a classwide basis, 'it is in fact rare to do so in advance of a motion for class certification' ").

As for Plaintiffs' argument that Disney's motion is premature, "[c]ourts generally conduct a choice of law analysis prior to the class certification stage unless plaintiffs show that further discovery is necessary for such an analysis." *Cimoli v. Alacer Corp.*, 587 F. Supp. 3d 978, 986 (N.D. Cal. 2022) (Freeman, J.). *Compare Doe v. Meta Platforms, Inc.*, No. 22-cv-03580 WHO, 2023 U.S. Dist. LEXIS 158683, at *16 (N.D. Cal. Sept. 7, 2023) (indicating that a choice-of-law analyses may be deferred until class certification, "after discovery shed[s] light on whether defendants' acts had a substantial nexus to California"), *with Davison v. Kia Motors Am., Inc.*, No. SACV 15-00239-CJC( ), 2015 U.S. Dist. LEXIS 85080, 2015 WL 3970502, at *2 n.3 (C.D. Cal. June 29, 2015) (stating that "many courts have decided against deferring the choice of law decision until discovery or class certification where, as here, the material differences [related to choice of law] are sufficiently obvious from the pleadings"). Here, Plaintiffs have not argued that the choice-of-law issue should be deferred so that they may conduct some discovery first. And the Court also bears in mind that there is a practical interest in resolving choice of law sooner rather than later – *i.e.*, otherwise, nationwide class discovery would be needed.

***17** Turning to the merits, the Court takes note that neither party has conducted a choice-of-law analysis. *See, e.g., In re Yahoo Mail Litig.*, 308 F.R.D. 577, 606 (N.D. Cal. 2015) (Koh, J.) (after conducting a choice-of-law analysis, denying plaintiffs' motion to certify a nationwide class as to their CIPA claim but certifying a California-only subclass as to that claim). At the hearing, however, Plaintiffs essentially conceded that a choice-of-law analysis would not run in their favor, particularly in light of the Ninth Circuit's decision *Mazza v. American Honda Motor Co.*, 666 F.3d 581 (9th Cir. 2012). There, the Ninth Circuit noted as follows:

> California recognizes that "with respect to regulating or affecting conduct within its borders, the place of the wrong has the predominant interest." California considers the "place of the wrong" to be the state where the last event necessary to make the actor liable occurred. *See McCann*, 48 Cal. 4th at 94 n.12, 105 Cal.Rptr.3d 378, 225 P.3d 516 (pointing out that the geographic location of an omission is the place of the transaction where it should have been disclosed); *Zinn v. Ex-Cell-O Corp.*, 148 Cal. App. 2d 56, 80 n.6, 306 P.2d 1017 (1957) (concluding in 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). Here, the 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.

Id. at 593-94.

Here, there is a strong argument that the last event necessary to make Disney liable was when Oracle (after being hired by Disney) intercepted the website users' communications. Plaintiffs arguably admit as much in their allegations related to the Pennsylvania claim. *See* Compl. ¶ 54 ("Plaintiff James's and Pennsylvania Subclass Members' electronic communications were intercepted in Pennsylvania, which is 'the point at which the signals [*i.e.*, Plaintiff's and the Pennsylvania Subclass's electronic communications] were routed to [Oracle's] servers.' ") (quoting *Popa II*, 52 F.4th at 130); *see also Popa II*, 52 F.4th at 130 ("NaviStone intercepted Popa's communications at the point where it routed those communications to its own servers. And that was at Popa's browser, not where the signals were received at NaviStone's servers.").

Accordingly, California law could apply nationwide only if California law did not materially differ from the law of other states. [9] In *Yahoo*, the district court found that there

> there are material differences between CIPA and the wiretapping statutes of the other 49 states. For example, some states expressly exclude email from their wiretapping statutes, others require only single party consent, and still others require plaintiffs to prove that they had either an objective or subjective expectation of privacy. These differences are material, as their application would "spell the difference between the success and failure of a claim." Moreover, there are also "material differences in the remedies given by state laws," as some states provide for injunctive relief while others do not, and the states vary as to whether damages may be recovered.

***18** *Yahoo*, 308 F.R.D. at 602-03.

9 Technically, California's choice-of-law test has three steps: (1) "whether the law of the other states is materially different from California law"; (2) "whether the other state has an interest in having its law applied"; and (3) "if another state has an interest, ... which state's interest would be most impaired if its policy were subordinated to the law of another state." *Yahoo*, 308 F.R.D. at 602. But practically speaking, (2) runs in Disney's favor based on the *Mazza* analysis above, and (3) essentially follows (2), thus leaving (1) as the remaining consideration.

In light of the analysis above, and Plaintiffs' concession that a nationwide class is not possible, the Court grants Disney's motion for relief. The nationwide class is dismissed and/or stricken. This leave Plaintiffs with a putative California class and a putative Pennsylvania class.

III. CONCLUSION

For the foregoing reasons, the Court denies the motion to dismiss for lack of standing. However, it dismisses or strikes the nationwide class, which leaves Plaintiffs with a putative California class and a putative Pennsylvania class. Finally, the Court grants in part and denies in part the motion to dismiss for failure to state a claim for relief. Plaintiffs have sufficiently pled its statutory claims, except to the extent they seek to hold Disney liable for Oracle's alleged interception of information for the use of *non*-Disney clients. Plaintiffs have leave to amend to cure this deficiency, if they can do so in good faith. Because the Court is giving Plaintiffs leave to amend here, it shall also permit Plaintiffs to provide more information about the mouse clicks and keystrokes allegedly intercepted (*i.e.*, to show that personal, non-record information was collected). Plaintiffs shall file their amended complaint within four weeks of the date of this order. If Plaintiffs do not file an amended complaint, then Disney shall file an answer to the complaint within six weeks of the date of this order.

This order disposes of Docket No. 15.

IT IS SO ORDERED.

All Citations

--- F.Supp.3d ----, 2023 WL 7392285