UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

DACIA THOMAS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

PAPA JOHNS INTERNATIONAL, INC., D/B/A PAPA JOHNS,

Defendant.

Case No.: 22cv2012 DMS (MSB)

ORDER GRANTING DEFENDANT'S MOTION TO DISMISS

On August 14, 2023, this Court granted in part and denied in part Defendant's motion to dismiss this case. (*See* ECF No. 26.) Specifically, the Court denied Defendant's motion to dismiss for lack of personal jurisdiction, and granted Defendant's motion to dismiss for failure to state a claim. Plaintiff's claim under California's Invasion of Privacy Act was dismissed without leave to amend, but the Court granted Plaintiff leave to amend to add specific facts to support her claim for invasion of privacy/intrusion upon seclusion. Following that Order, Plaintiff filed a Second Amended Complaint realleging her intrusion upon seclusion claim. Defendant now moves to dismiss that claim with prejudice, or at a minimum, to dismiss Plaintiff's requests for injunctive and equitable relief.

As stated in the Court's previous order, a claim for intrusion upon seclusion has two elements. "First, the defendant must intentionally intrude into a place, conversation, or

matter as to which the plaintiff has a reasonable expectation of privacy. Second, the intrusion must occur in a manner highly offensive to a reasonable person." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009). Defendant argues primarily that Plaintiff has failed to allege sufficient facts to support the elements of a "reasonable expectation of privacy" and an intrusion "highly offensive to a reasonable person."[1]

"A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms." *Hill v. NCAA*, 7 Cal. 4th 1, 37 (1994). Whether an expectation of privacy is "reasonable" depends on the circumstances of each case. *Id.* at 36. Those circumstances include the "customs, practices, and physical setting" surrounding the activity, whether there was advance notice of any impending action, whether there was an opportunity to give voluntary consent, *id.* at 36-37, the identity of the intruder, and the nature of the intrusion. *Hernandez*, 47 Cal. 4th at 289. Other relevant factors include "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*, 615 F.Supp.3d 1069, 1088 (N.D. Cal. 2022). Although whether a plaintiff has a reasonable expectation of privacy is generally a mixed question of law and fact, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020), "[i]f the undisputed material facts show no reasonable expectation of privacy …, the question of invasion may be adjudicated as a matter of law." *Hill*, 7 Cal. 4th at 40.

Here, Plaintiff alleges she was browsing and using Defendant's public website. (SAC ¶ 8.) Generally, the internet is not a place where users have a reasonable expectation of privacy. As stated in *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 266 (3d Cir. 2016):

---

[1] Defendant also argues Plaintiff has failed to plead a legally protected privacy interest, and Plaintiff is not entitled to seek relief in equity. In light of the discussion below on the "reasonable expectation of privacy" and "highly offensive" elements, the Court declines to address Defendant's other arguments.

> Most of us understand that what we do on the Internet is not completely private. How could it be? We ask large companies to manage our email, we download directions from smartphones that can pinpoint our GPS coordinates, and we look for information online by typing our queries into search engines. We recognize, if only intuitively, that our data has to be going somewhere. And indeed it does, feeding an entire system of trackers, cookies, and algorithms designed to capture and monetize the information we generate.

Given the inherent nature of the internet, a number of courts have found that consumers do not have a reasonable expectation of privacy over their activity in that space. *See D'Angelo v. Penny OpCo, LLC*, No. 23-cv-0981-BAS-DDL, 2023 WL 7006793, at *10-11 (S.D. Cal. Oct. 24, 2023) (stating "accepted community norms around conversations in this type of space (a commercial website for selling merchandise) point away from a reasonable expectation of privacy."); *Saleh v. Nike, Inc.*, 562 F.Supp.3d 503, 524-25 (C.D. Cal. 2021) (agreeing with defendants that plaintiff did not have "a reasonable expectation of privacy over his activity on Nike's Website"); *Saeedy v. Microsoft Corp.*, No. 23-cv-1104, 2023 WL 8828852, at *4 (W.D. Wash. Dec. 21, 2023) (stating "mouse movements, clicks, keystrokes, keywords, URLs of web pages visited, product preferences, interactions on a website, search words typed into a search bar, user/device identifiers, anonymized data, product selections to a shopping cart, and website browsing activities" are not the types of information in which plaintiffs could have "a reasonable expectation of privacy"); *Farst v. AutoZone, Inc.*, ___ F.Supp.3d ___, 2023 WL 7179807, at *4 (M.D. Penn. Nov. 1, 2023) ("Shopping on a public website, like shopping in a public store, is not an activity one can reasonably expect to keep private from the retailer."); *Massie v. General Motors LLC*, No. 21-787-RGA, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022) (stating plaintiffs did not have a reasonable expectation of privacy over anonymized data captured by Session Replay software); *see also Campbell v. Facebook Inc.*, 77 F.Supp.3d 836, 849 (N.D. Cal. 2014) ("California appeals courts have generally found that Internet-based communications are not 'confidential' within the meaning of section 632, because such communications can easily be shared by, for instance, the recipient(s) of the communications."); *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *22-23 (N.D. Cal. Sept. 26, 2013)

(granting motion to dismiss claims under California Penal Code § 632 because instant messages were not "confidential"); *Cook v. GameStop, Inc.*, ___ F.Supp.3d ___, 2023 WL 5529772, at *6-10 (W.D. Penn. Aug. 28, 2023), *appeal filed*, No. 23-2574 (3d Cir. Aug. 29, 2023) (explaining why mouse movements and clicks, URLs, and keystrokes are not protected under Pennsylvania's Wiretap Act).

This is not to say there can never be a reasonable expectation of privacy over internet activity. For instance, courts have found users have a reasonable expectation of privacy if a company states it will not collect your information in certain spaces or while searching in a protected mode. *See In re Facebook*, 956 F.3d at 601-03 (finding users had reasonable expectation of privacy in activity outside of application where privacy policy stated defendant would not collect user data after user had logged out); *Brown v. Google LLC*, ___ F.Supp.3d ___, 2023 WL 5029899, at *19-20 (N.D. Cal. Aug. 7, 2023) (finding plaintiffs had reasonable expectation of privacy when browsing in private or incognito mode); *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 630 (N.D. Cal. 2021) (finding plaintiffs "had a reasonable expectation of privacy in the data allegedly collected" based on defendant's representations that it would not receive user data while they were not synced).

In each of these cases, *In re Facebook*, *Brown*, and *Calhoun*, the plaintiffs pleaded specific facts concerning the factors sets out above, i.e., the customs, practices and circumstances surrounding the defendant's particular activities, the amount and sensitivity of the data collected, and the manner of data collection. In *In re Facebook*, for instance, the plaintiffs attached to their complaint copies of certain "Help Center" pages regarding the defendant's data tracking practices. 956 F.3d at 602. *See also In re Nickelodeon*, 827 F.3d at 269 (including allegations that defendant's registration form disclaimed that any data was collected from plaintiff's kids); *Calhoun*, 526 F.Supp.3d at 614 (detailing allegations about defendant's data collection practices); *Brown*, 2023 WL 5029899, at *2 (same). They also included specifics about the amount and sensitivity of the data the defendants were allegedly collecting. *See In re Facebook*, 956 F.3d at 603 (describing

"enormous amount of individualized data" collected by defendant); *Calhoun*, 526 F.Supp.3d at 613-14 (detailing amount and nature of personal information defendant collected).

Here, Plaintiff describes the general circumstances surrounding Defendant's activities, namely, its procurement of Session Replay Providers to embed Session Replay Code on its website, and how Session Replay Code generally works. (SAC ¶¶ 24-44.) Plaintiff also identifies one of Defendant's specific Session Replay Providers, FullStory, and sets out further details about how its Session Replay Code, FullStory Script, works. (*Id.* ¶¶ 47-49.) Plaintiff further alleges that her "Website Communications"[2] with Defendant were secretly "captured by Session Replay Code and sent to various Session Replay Providers." (*Id.* ¶ 60.)

Notably absent from the SAC are any specific allegations about the customs and practices related to Defendant's activities. However, the numerous cases filed in federal courts around the country challenging the use of Session Replay Code suggest Defendant is not alone in this practice. *See Mikulsky v. Noom, Inc.*, No. 3:23-cv-00285-H-MSB, 2024 WL 251171, at *1 (S.D. Cal. Jan. 22, 2024) (noting the "dozens of proposed class actions being litigated in federal courts challenging the use of 'Session Replay Code.'"); *In re TikTok, Inc., Consumer Privacy Litig.*, ___ F.Supp.3d ___, 2024 WL 278987, at *7 n.8 (N.D. Ill. Jan. 25, 2024) (stating session replay code "is widely used by website operators and app developers to track and record how users interact with digital platforms."); *see also Popa v. PSP Group, LLC*, No. C23-0294JLR, 2023 WL 7001456, at *1 (W.D. Wash. Oct. 24, 2023) (listing "dozens of proposed class actions being litigated in federal court

---

[2] The SAC defines "Website Communications" as "electronic communications with the Papa Johns website, [her] mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time[.]" (*Id.* ¶ 1.) Plaintiff also alleges "Website Communications" include "her name, home address, credit card number(s), and billing information." (*Id.* ¶ 56.)

across the country challenging the use of 'Session Replay Code' to record, save, analyze, and replay internet users' interactions with consumer websites."); *Jones v. Papa John's Int'l, Inc.*, No. 4:23-cv-00023-SRC, 2023 WL 7155562, at *1 (E.D. Missouri Oct. 31, 2023) ("This is one of many lawsuits challenging the use of 'session replay code' that companies such as Papa John's say helps improve the user experience on their websites by monitoring user activity."); *Cook*, ___ F.Supp.3d ___, 2023 WL 5529772, at *1 (same). Standing alone, this does not mean Plaintiff did not have a reasonable expectation of privacy over her "Website Communications" on Defendant's website, but it is a factor to consider in making that determination. *See In re Facebook*, 956 F.3d at 601-02 (quoting *Hernandez*, 47 Cal. 4th at 286) (stating reasonable expectation of privacy inquiry considers "whether a defendant gained 'unwanted access to data by electronic or other covert means, in violation of the law or social norms.'"); *Hill*, 7 Cal. 4th at 24-25 (stating common law invasion of privacy is concerned "with aspects of life consigned to the realm of the 'personal and confidential' by strong and widely shared social norms.")

Another factor is the amount and sensitivity of any data collected. Here, Plaintiff alleges Defendant collected users' "Website Communications," which, by definition, are limited to Defendant's website. This limited amount of data stands in stark contrast to the "significant" amounts of data collected in other cases. *See In re Facebook*, 956 F.3d at 603 (stating defendant "acquires an 'enormous amount of individualized data' through its use of cookies on the countless websites that incorporate Facebook plug-ins."); *Calhoun*, 526 F.Supp.3d at 630 (noting that defendant's code was used on 86 percent of popular websites); *Brown*, 2023 WL 5029899, at *20 (stating amount of data collected was "indisputably vast").

The type of data allegedly collected in this case also pales in comparison to the type of data collected in other cases. In those cases, the data collected included "the user's browsing history, including the identity of the individual internet user and the web servers, as well as the name of the web page and the search terms that the user used to find it[,]" *In re Facebook*, 956 F.3d at 596, which enabled the defendant to compile "cradle-to-grave"

profiles without the users' consent. *Id.* at 599. Those 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. See also Katz-Lacabe v. Oracle America, Inc.*, 668 F.Supp.3d 928, 942 (N.D. Cal. 2023) (allegation that defendant collected "sensitive health and personal safety information" was sufficient to withstand motion to dismiss claim for intrusion upon seclusion).

Here, the data allegedly collected includes Plaintiff's "electronic communications with the Papa Johns website, [her] mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time[.]" (SAC ¶ 1.) As for Plaintiff's web chats or emails on Defendant's website, case law is relatively clear that it is not objectively reasonable to expect those communications to be private. *See D'Angelo*, 2023 WL 7006793, at *10-11 (S.D. Cal. Oct. 24, 2023) (stating it would not be reasonable for a consumer to expect privacy over chats on a public website); *In re Yahoo Mail Litig.*, 7 F.Supp.3d 1016, 1041 (N.D. Cal. 2014) ("to the extent Plaintiffs claim they have a legally protected privacy interest and reasonable expectation of privacy in email *generally*, regardless of the specific content in the emails at issue, Plaintiffs' claim fails as a matter of law."); *In re Google Inc.*, 2013 WL 5423918, at *22-23 (granting motion to dismiss claims under California Penal Code § 632 because instant messages were not "confidential"). This is because these communications "are by their very nature recorded on the computer of at least the recipient, who may then easily transmit the communication to anyone else who has access to the internet or print the communications." *Id.* at *23; *see also Campbell*, 77 F.Supp.3d at 849 ("California appeals courts have generally found that Internet-based communications are not 'confidential' within the meaning of section 632, because such communications can easily be shared by, for instance, the recipient(s) of the communications.")

/ / /

Next are Plaintiff's "mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), [and] URLs of web pages visited[.]" (SAC ¶ 1.) As with the communications discussed above, a number of courts have found this type of information is not something over which a consumer has an objectively reasonable expectation of privacy. *See Saleh*, 562 F.Supp.3d at 524-25 (agreeing with defendants that plaintiff did not have "a reasonable expectation of privacy over his activity on Nike's Website"); *Saeedy*, 2023 WL 8828852, at *4 (stating "mouse movements, clicks, keystrokes, keywords, URLs of web pages visited, product preferences, interactions on a website, search words typed into a search bar, user/device identifiers, anonymized data, product selections to a shopping cart, and website browsing activities" are not the types of information in which plaintiffs could have "a reasonable expectation of privacy"); *Cook*, ___ F.Supp.3d ___, 2023 WL 5529772, at *6-10 (explaining why mouse movements and clicks, URLs, and keystrokes are not protected under Pennsylvania's Wiretap Act). *See also Massie*, 2022 WL 534468, at *5 (stating plaintiffs did not have a reasonable expectation of privacy over anonymized data captured by Session Replay software); *Farst*, ___ F.Supp.3d ___, 2023 WL 7179807, at *4 ("Shopping on a public website, like shopping in a public store, is not an activity one can reasonably expect to keep private from the retailer.")

The only other specific information identified as "Website Communications" is Plaintiff's "name, address, credit card number(s), and billing information." (SAC ¶ 56.) Reading that information in context, it appears Plaintiff entered this information on Defendant's website in connection with ordering "take-out and/or delivery of food from Papa Johns' brick and mortar stores located in California." (*Id.* ¶ 8.) This information is similar to Plaintiff's web chats and emails, and is not information over which society is prepared to recognize a reasonable expectation of privacy "because 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'" *United States v. Forrester*, 512 F.3d 500, 509 (9th Cir. 2008) (quoting *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)).

The type of data allegedly collected here is also a far cry from the type of data that supports a finding of a reasonable expectation of privacy. *See Opperman v. Path, Inc.*, 87 F.Supp.3d 1018, 1060 (N.D. Cal. 2014) (address books); *Thompson v. Spitzer*, 90 Cal. App. 5th 436, 460 (2023) (DNA and genetic information); *Murchison v. County of Tehama*, 69 Cal. App. 5th 867, 883 (2021) (private homes*); County of Los Angeles v. Superior Court*, 65 Cal. App. 5th 621, 643 (2021) (medical records); *Chantiles v. Lake Forest II Master Homeowners Assn.*, 37 Cal. App. 4th 914, 924 (1995) (voting information); *Doyle v. State Bar*, 32 Cal. 3d 12, 19 (1982) (financial information).

The only factor that possibly supports a finding of a reasonable expectation of privacy in this case is the notice factor. On that factor, Plaintiff alleges Defendant secretly embedded Session Replay Codes on its website, (SAC at 12), which removed any opportunity for Plaintiff to consent to the interception and recording of her "Website Communications."[3] However, given the other circumstances and factors discussed above, Defendant's alleged failure to give notice, in and of itself, does not give rise to a reasonable expectation of privacy in users' "Website Communications." *See D'Angelo*, 2023 WL

---

[3] It is unclear when Plaintiff allegedly visited Defendant's website, but if her visits occurred between December 19, 2020, and December 19, 2022, Defendant's Privacy Policy then in effect would contradict Plaintiff's allegation that Defendant secretly embedded Session Replay Code on its website. (*See* Decl. of Joshua Hall in Supp. of Mot. ¶¶ 5-6.) That Policy was linked on every page of Defendant's website, (*id.* ¶ 6), and would have alerted Plaintiff to the possibility that third parties were monitoring her interactions with Defendant's website. *See* https://tinyurl.com/ymr8af7p ("We use tracking tools like browser cookies and web beacons. To learn more about these tools and how you can control them, click here. We collect information about users over time when you use this website. *We may have third parties collect personal information this way*. We also collect information from our mobile apps.") (emphasis added). That Policy is subject to judicial notice, *see Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005) (stating incorporation by reference doctrine "applies with equal force to internet pages as it does to printed material."), and would rebut any presumption of truth applicable to Plaintiff's allegations. *See Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001) (stating court need not accept as true "allegations that contradict matters properly subject to judicial notice").

7006793, at *11 (stating factors "point away from a reasonable expectation of privacy" even though plaintiffs did not have advance notice or provide consent to defendant's activities).

Plaintiff's allegations about the reasonable expectations of privacy of website users, (SAC ¶ 19) (alleging "website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated."), the reasonable expectations of privacy of visitors to Defendant's website, (*id.* ¶ 53) (alleging "Papa Johns' customers, such as Plaintiff, reasonably expect their conversations with Papa Johns via its website to be private and not shared with third parties. Moreover, they reasonably expect their potential conversations that they type into a chatbox on Papa Johns' website that they never share (such as by deleting before clicking 'send') to be private. Finally, they reasonably expect mouse movements and other resizing and scrolling to be private."), and her own subjective expectations of privacy while she was on Defendant's website, (*id.* ¶ 47) (alleging Plaintiff "had a reasonable expectation of privacy in [her] Website Communications specifically including but not limited to the expectation that Defendant would not disclose and/or provide this information to third parties, including the Session Replay Providers.") are also insufficient to satisfy the "reasonable expectation of privacy" element. All of these allegations are either general and conclusory, and therefore not entitled to a presumption of truth, *Ashcroft v. Iqbal*, 556 U.S. 662, 681 (2009), or irrelevant to whether visitors to Defendant's website had an objectively reasonable expectation of privacy in their "Website Communications." *See Shulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 232 (1998) (stating tort of intrusion upon seclusion "is proven only if the plaintiff had an *objectively* reasonable expectation of seclusion or solitude in the place, conversation or data source.") (emphasis added).

Considering the factors and allegations discussed above, both alone and in combination, Plaintiff has failed to allege sufficient, specific facts to support the "reasonable expectation of privacy" element of her claim.

/ / /

The only other element of Plaintiff's claim is an intrusion that is "highly offensive to a reasonable person." Before addressing the parties' substantive arguments on this element, the Court first addresses Plaintiff's argument that this issue cannot be resolved on the present motion. In support of this argument, Plaintiff relies on *In re Facebook*, where the court stated the question of whether the defendant's data collection practices "could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage." *In re Facebook*, 956 F.3d at 606. Subsequent cases, however, have not read that statement so broadly. Indeed, some courts have interpreted that statement as limited to the facts of that case. *See James v. Allstate Ins. Co.*, No. 3:23-cv-01931-JSC, 2023 WL 8879246, at *6 (N.D. Cal. Dec. 22, 2023); *Williams v. DDR Media, LLC*, No. 22-cv-03789-SI, 2023 WL 5352896, at *5-6 (N.D. Cal. Aug. 18, 2023). And those courts are not alone in resolving the issue on the basis of the pleadings. *See Cousin v. Sharp Healthcare*, 681 F.Supp.3d 1117, 1126-27 (S.D. Cal. 2023); *Hammerling*, 615 F.Supp.3d at 1090-91; *Mastel v. Miniclip SA*, 549 F.Supp.3d 1129, 1139-42 (E.D. Cal. 2021); *In re Google, Inc. Privacy Policy Litig.*, 58 F.Supp.3d 968, 987-99 (N.D. Cal. 2014); *Low v. LinkedIn Corp.*, 900 F.Supp.2d 1010, 1024-26 (N.D. Cal. 2012).

The *Mastel* court's reasoning on this issue is particularly persuasive. There, the court looked to California Supreme Court decisions involving invasion of privacy claims under the California Constitution, namely *Hill* and *Loder v. City of Glendale*, 14 Cal. 4th 846 (1997), both of which "provided some clear and objective guidance as to the trial courts' role in applying [the term 'highly offensive'] at the pleading stage." *Mastel*, 549 F.Supp.3d at 1140. That guidance instructs "that courts have a role to play in 'weed[ing] out claims that involve so insignificant or de minimus an intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant.'" *Id.* (quoting *Loder*, 14 Cal. 4th at 893). As stated in *Hill*, "'No community could function if every intrusion into the realm of private action, no matter how slight or trivial, gave rise to a cause of action for invasion of privacy.'" *Id.* (quoting *Hill*, 7 Cal. 4th

/ / /

at 41). Based on this reasoning, and in light of the dispute over the language in *In re Facebook*, this Court will address the "highly offensive" element here.

The "highly offensive" element "essentially involves a 'policy' determination as to whether the alleged intrusion is 'highly offensive' under the particular circumstances." *Hernandez*, 47 Cal. 4th at 287 (citing *Taus v. Loftus*, 40 Cal. 4th 683, 737 (2007)). "Relevant factors include the degree and setting of the intrusion, and the intruder's motives and objectives[,]" *id.* (citations omitted), the likelihood of serious harm to the victim, and whether countervailing interests or social norms render the intrusion inoffensive. *Hammerling*, 615 F.Supp.3d at 1090 (quoting *In re Facebook*, 956 F.3d at 606).

Here, Plaintiff addresses some of these factors in her SAC. (*See* SAC ¶¶ 83, 89) (alleging Defendant utilized information gathered for "business gain" and "economic value"); (*id.* ¶¶ 86-87) (alleging Defendant's conduct caused "mental anguish and suffering," and "emotional distress, worry, fear, and other harms.") But again, Plaintiff's allegations are general and conclusory. Plaintiff provides more specific allegations on the degree of the intrusion factor, (*see id.* ¶ 36) (alleging Session Replay Provider can create "fingerprints" from information "collected across all sites that the Session Replay Provider monitors[,]") but she fails to allege the Session Replay Provider or Providers procured by Defendant actually collected that kind of "fingerprint" information from Plaintiff or any other visitor to Defendant's website. Plaintiff's other allegations directed to the "highly offensive" element are conclusory, (*see id.* ¶ 41 ("Papa Johns' procurement of Session Replay Providers to surreptitiously and instantaneously record every Website Communication is highly offensive[.]"); *see also id.* ¶ 54 (same)), and do not defeat Defendant's motion. *See Oregon Clinic, PC v. Fireman's Fund Ins. Co.*, 75 F.4th 1064,

/ / /

/ / /

/ / /

/ / /

/ / /

1073 (9th Cir. 2023) ("conclusory allegations, without more, are insufficient to defeat a motion to dismiss.")[4]

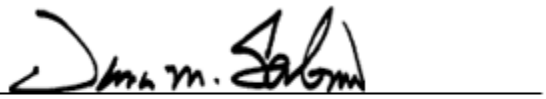
III.

CONCLUSION

In light of the above discussion, the Court finds Plaintiff has failed to allege sufficient, specific facts to support either the "reasonable expectation of privacy" or "highly offensive" prongs of her intrusion upon seclusion claim. Accordingly, the Court grants Defendant's motion to dismiss and dismisses this case with prejudice. The Clerk of Court shall enter judgment accordingly and close this case.

IT IS SO ORDERED.

Dated: May 8, 2024



Hon. Dana M. Sabraw, Chief Judge
United States District Court

[4] Even if the Court assumed all of Plaintiff's allegations were true, those allegations would be sufficient to support the "highly offensive" element. *See Doe v. Kaiser Foundation Health Plan, Inc.*, No. 23-cv-02865-EMC, 2024 WL 1589982, at *18-19 (N.D. Cal. Apr. 11, 2024) (stating it was not clear that defendant's employment of third party to collect information about website users for defendant's benefit was "highly offensive to a reasonable person"); *Popa v. Harriet Carter Gifts, Inc.*, 426 F.Supp.3d 108, 122-23 (W.D. Penn. 2019) ("The act of collecting Popa's keystrokes, mouse clicks, and [Personally Identifiable Information] is simply not the type of highly offensive act to which liability can attach."); *see also Cousin*, 681 F.Supp.3d at 1126-27 ("disclosing a user's browsing history does not plausibly reach the level of 'highly offensive' conduct under either the common law or the California Constitution.").