

United States District Court
Northern District of California

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

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

FLORENTINO JAVIER,
Plaintiff,
v.
ASSURANCE IQ, LLC, et al.,
Defendants.

Case No. 4:20-cv-02860-JSW

**ORDER GRANTING MOTION TO
DISMISS**

Re: Dkt. No. 28

Now before the Court is defendants’ motion to dismiss the first amended complaint. (Dkt. No. 28 (“MTD”).) The Court has considered the parties’ papers, relevant legal authority, and the record in this case, and it finds the motion suitable for disposition without oral argument. See N.D. Civ. L.R. 7-1(b). The Court GRANTS defendants’ motions to dismiss.

BACKGROUND

Plaintiff Florentino Javier (“Javier”) brings this purported consumer privacy class action against defendants Assurance IQ, LLC (“Assurance”) and ActiveProspect Inc. (“ActiveProspect”) (together, “Defendants”) for violation of the California Invasion of Privacy Act (“CIPA”), Cal. Penal Code § 631, and the California Constitution based on surreptitious recording of user actions on Assurance’s website. The complaint alleges as follows. (Dkt. No. 24 (“FAC”).)

Assurance is an online platform for life insurance quotes. (*Id.* ¶ 6.) Assurance runs a website called Nationalfamily.com that allows persons to obtain life insurance quotes. (*Id.* ¶ 9, 40.) A user enters information about her demographics, family situation, and medical history, and then clicks “View My Quote.” (*Id.* ¶¶ 33-39.) At the final step, the website states that by clicking “View my Quote,” the user provides an “electronic signature as an indication of . . . intent to agree to the website’s Privacy Policy” and “Terms of Service.” (*Id.* ¶ 39.) This is shown below:

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

National Family
ASSURANCE CORPORATION

Call an Agent

Last step! Your quote is ready.

Florentino

Javier

(408) [REDACTED]

[REDACTED]@gmail.com

View My Quote >

By clicking 'View My Quote', I provide my electronic signature as an indication of my intent to agree to this website's [Privacy Policy](#), [Terms of Service](#), and expressly

Assurance partners with ActiveProspect for its website. (*Id.* ¶¶ 23-26.) ActiveProspect provides “TrustedForm,” which is a “lead certification product that helps businesses comply with regulations like the Telephone Consumer Protection Act . . . by documenting consumer consent.” (*Id.* ¶ 12 (internal brackets and quotation marks omitted).) Specifically, TrustedForm is a piece of javascript code that can be pasted into a form page to record “keystrokes, mouse clicks, data entry, and other electronic communications of visitors to websites.” (*Id.* ¶¶ 20-21.) As the result, a website owner can record a video of a users’ interaction on its website, including consent to being contacted by phone. (*Id.* ¶¶ 18-19.)

Javier visited Assurance’s website on January 2019. (*Id.* ¶ 30.) He entered all of the required information, including health data, and presumably obtained a life insurance quote. (*Id.* ¶¶ 33-39.) A few months later, Javier sent a letter through counsel to an unnamed company “over purported violations of the Telephone Consumer Protection Act.” (*Id.* ¶ 46.) The company then produced a recording of him consenting to being contacted by phone. (*Id.*) Javier was “shocked to discover” that his activities had been recorded on Assurance’s website, and brought this lawsuit the same month. (*Id.* ¶ 47.)

ANALYSIS

A. Legal Standard.

Defendants move to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6). Dismissal under Rule 12(b)(6) is granted when the pleadings fail to state a claim upon which relief can be granted. Pursuant to *Bell Atlantic v. Twombly*, a plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” 550 U.S. 544, 570 (2007). “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.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). If the allegations are insufficient to state a claim, a court should grant leave to amend, unless amendment would be futile. *See Reddy v. Litton Indus., Inc.*, 912 F.2d 291, 296 (9th Cir. 1990). Where a plaintiff alleges fraud, Rule 9(b) requires the plaintiff to state the circumstances constituting fraud with particularity. *See Fed. R. Civ. P. 9(b)*. Particularity under Rule 9(b) requires the plaintiff to plead the “who, what, when, where, and how” of the misconduct. *See Kearns v. v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009).

B. The Court Grants Defendants’ Motion to Dismiss.

Defendants move to dismiss on the grounds that Javier consented to having his information collected on Assurance’s website. Consent generally defeats privacy claims. That is because a party that consents to having information collected has no reasonable expectation of privacy. *See Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016). CIPA expressly requires “unauthorized” conduct or conduct “without the consent of all parties.” Cal. Penal Code § 631. The California Constitution similarly requires that “the plaintiff’s expectations of privacy . . . be reasonable.” *Hernandez v. Hillside, Inc.*, 47 Cal. 4th 272, 287 (2009); *see also Hill v. Nat’l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 26 (1994) (no “egregious” intrusion with consent).

That said, consent “is not an all-or-nothing proposition.” *In re Google*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013). “There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law.” *Sanders v. Am. Bd. Co., Inc.*, 20 Cal. 4th 907, 916 (1999). Consent is therefore generally

1 limited to the specific conduct authorized. *See, e.g., Campbell v. Facebook Inc.*, 77 F. Supp. 3d
 2 836, 847 (N.D. Cal. 2014) (no consent to data being used for targeted advertising where users
 3 consented to its use for “data analysis”); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d
 4 797, 824 (N.D. Cal. 2020) (consent to data collection does not extend to data disclosure). Consent
 5 is frequently evaluated using principles of contract to determine “whether the user ‘agreed’” to the
 6 specific use or collection. *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F.
 7 Supp. 3d 767, 789 (N.D. Cal. 2019).

8 Here, the parties do not dispute that Javier affirmatively clicked on “View My Quote” on
 9 Assurance’s website to indicate “intent to agree to th[e] website’s Privacy Policy.” (FAC ¶ 39.)

10 The privacy policy, which is subject to judicial notice,¹ states:

11 We collect the content and other personal information that may be
 12 used to identify you as an individual you provide when you use our
 13 Services, including when you request an insurance quote, apply for
 14 insurance, and sign up for an account. This can be personally
 15 identifiable information, health information, and information about
 16 property you own or lease. We also collect information about how
 17 you use our Services, such as the types of content you view or engage
 18 with or the frequency and duration of your activities.

19 The personal information we may collect includes, but is not limited
 20 to: name, address, date of birth, phone number, email address, height,
 21 weight, social security number, vehicle details, personal and family
 22 health information

23 We may use third party vendors to assist us with the Service. Some
 24 examples of the assistance that may be provided by third party service
 25 providers are: monitoring and analyzing Site activity, operations and
 26 marketing, hosting the Site, and maintaining our database.

27 By submitting your personal information either to us or to any of your
 28 partners, you consent to the use of your personal information as set
 forth above, and to the transfer of that data to our partners or those
 individuals or entities we engage to provide Services in connection
 with your transaction.

(Dkt. No. 28-4 at 4 (“Privacy Policy”).)

¹ The privacy policy is properly subject to judicial notice because it is publicly available on Defendants’ website and Javier does not question its authenticity. *See Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 814; *Opperman*, 205 F. Supp. 3d at 1068 n.3.

1 Defendants argue that this Privacy Policy discloses each action that Javier now challenges
2 as intrusive, including: collection of sensitive information (“We collect . . . health information”),
3 monitoring of website activity (“We also collect information about how you use our Services, such
4 as the types of content you view or engage with or the frequency and duration of your activities”),
5 use of ActiveProspect (“We may use third party vendors to assist us with the Service,” including
6 “monitoring and analyzing Site activity”), and data sharing with ActiveProspect (“[Y]ou consent
7 to . . . the transfer of that data to . . . entities we engage to provide Services”). However, Javier
8 argues that his consent was invalid because (1) it occurred after the alleged privacy invasion took
9 place, (2) Javier lacked sufficient notice of the privacy policy, and (3) the privacy policy did not
10 disclose the exact conduct at issue.

11 With respect to the first issue, the Court has found no case addressing retroactive consent
12 in the privacy context.² However, outside of privacy law, California courts frequently uphold
13 retroactive consent as valid. *See, e.g., Salgado v. Carrows Rest., Inc.*, 33 Cal. App. 5th 356, 361
14 (2019) (rejecting the claim that agreement to arbitrate “must pre-date the actions giving rise to the
15 dispute” as “contrary to contract principles”); *Franco v. Greystone Ridge Condominium*, 39 Cal.
16 App. 5th 221, 230 (2019) (similar). These cases do not require express language specifying that
17 consent extends retroactively, as long as there is no time “limitation or restriction” on the claims.
18 *See Franco*, 39 Cal. App. 5th at 230. The privacy policy here is phrased in present tense—“we
19 collect” data when “you use our Services,” not “we will collect”—and thus gives fair notice that
20 Javier consents to actions that may have already taken place. Accordingly, on these facts, the
21 Court finds Javier’s retroactive consent to data collection valid.³

22 _____
23 ² Javier cites two inapposite cases concerning the Illinois Biometric Information Privacy Act,
24 which was specifically enacted to protect against the “difficulty of ‘un-disclosing’ biometric
25 information,” *Cothron v. White Castle System, Inc.*, 467 F. Supp. 3d 604, 617 (N.D. Ill. June 16,
26 2020), and confusing consent screens, where the terms and conditions appeared after the user may
reasonably conclude to have agreed to them. *Kauders v. Uber Techs., Inc.*, SUCV20162180D,
2019 WL 510568, at *5 (Mass. Super. Ct. Jan. 3, 2019)

27 ³ That is not to say that retroactive consent will always be valid. The data collection here occurred
28 mere minutes and seconds before Javier gave consent during a single website visit. The Court
does not address facts not before it, such as where data was collected months or weeks before.

1 With respect to the sufficiency of notice, Javier’s argument is meritless. The agreement
2 here is “clickwrap,” not “browsewrap,” which courts routinely uphold as valid. *See, e.g., Holl v.*
3 *United Parcel Serv., Inc.*, No. 16-cv-05856-HSG, 2017 WL 11520143, at **3-5 (N.D. Cal. Sept.
4 18, 2017); *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1165 (N.D. Cal.
5 2016); *Swift v. Zynga Game Network, Inc.*, 805 F. Supp. 2d 904, 910-12 (N.D. Cal. 2011)). Even
6 though the button that Javier pressed used different verbiage—“View My Quote,” instead of “I
7 agree”—the Ninth Circuit has upheld similar cases where a user affirmatively indicated assent.
8 *See Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014). Indeed, the agreement
9 here is similar to the one in *Facebook Biometric Information Privacy Litigation*, where a user
10 indicated assent by clicking “Register Now,” which had a hyperlink to the terms and conditions
11 below. *See* 185 F. Supp. 3d at 1162-63; *see also Dohrmann v. Intuit, Inc.*, 823 F. App’x 482, 484
12 (9th Cir. 2020) (upholding consent through notice below a “Sign In” button).

13 Javier dissects the details of the consent page, including the use of light blue letters and
14 lack of underlining, to argue that he lacked notice, but this argument largely misses the point. The
15 adequacy of notice must ultimately be evaluated holistically, not through mechanical application
16 of formatting rules.⁴ Here, the webpage on which Javier provided consent was uncluttered, with
17 only a few entry fields followed by the disclosure on a single page; the text placed hyperlinks in a
18 different color to indicate their selectability; and there were no additional features, such as a dark
19 background or additional links having different formatting, that would have obscured the notice.
20 On similar facts, courts have frequently found notice sufficient. *See Peter v. DoorDash, Inc.*, 445
21 F. Supp. 3d 580, 585-87 (N.D. Cal. 2020) (discussing cases). Viewed holistically, the clean and
22 uncluttered page by which Javier affirmatively consented, while having full ability and immediate
23 opportunity to read the privacy policy, shows that he had sufficient notice.

24 Last, with respect to the substance of the Privacy Policy’s disclosure, Javier argues that the
25 policy does not disclose recording because it places some disclosures in the “Web beacons”
26 section, instead of the “cookies and tracking technology” section; because the tracking technology

27 _____
28 ⁴ In any case, as explained by Defendants, courts have found notice adequate without any of the
features cited by Javier. (*See* Dkt. No. 28 (“MTD”) at 8:22-9:24.)

1 section indicates that tracking is performed “to enhance your shopping experience”; because the
 2 policy states Assurance “may” use third party monitors; and because “transfer [] of data” does
 3 indicate real time monitoring. These arguments are largely irrelevant. The policy clearly indicates
 4 that Assurance tracks activity on its website and may use third party vendors to do so. The policy
 5 as a whole is only two pages long, which means that none of the terms are buried or obscured.
 6 That the privacy policy also discusses other types of tracking, such as data collection for purposes
 7 of personalization, does not detract from its plain disclosures elsewhere. Accordingly, the Court
 8 finds that the privacy policy to which Javier agreed disclosed the specific conduct at issue here.

9 For the foregoing reasons, the Court dismisses Javier’s claims based on consent.⁵

10 CONCLUSION

11 For the foregoing reasons, the Court GRANTS Defendants’ motion to dismiss. The Court
 12 grants Javier leave to amend, if he can do so in good faith and in compliance with his obligations
 13 under Federal Rule of Civil Procedure 11 having considered the conclusions reached in this Order.
 14 Javier shall file and serve an amended complaint or a statement that no such amended complaint
 15 shall be filed within twenty days of the date of this Order, and Defendants shall file their response
 16 within twenty days thereafter.

17
 18 **IT IS SO ORDERED.**

19 Dated: March 9, 2021



20
 21 JEFFREY S. WHITE
 United States District Judge

22
 23
 24 _____
 25 ⁵ Defendants also move to dismiss for failure to state a claim because Assurance was a party to the
 26 communications and its collection of data for the purpose of providing life insurance quotes was
 27 not an “egregious” violation of social norms. Javier opposes by arguing that secret recording by a
 28 third-party, ActiveProspect, could satisfy these elements. However, that is not what the complaint
 alleges. Javier alleges that Assurance itself collects the information by pasting TrustedField
 javascript into its form page, which acts “as a hidden field.” (FAC ¶ 20.) Because the complaint
 never alleges that ActiveProspect itself every recorded or received his data, only that it provided
 a product by which Assurance did so, his opposition misses the mark. The complaint is therefore
 further dismissed for failure to state a claim.