

1
2
3
4
5
6
7
8 UNITED STATES DISTRICT COURT
9 SOUTHERN DISTRICT OF CALIFORNIA
10

11 MIGUEL ESPARZA, individually and on
12 behalf of all others similarly situated,
13 Plaintiff,
14 v.
15 KOHL'S, INC., a Delaware corporation,
16 d/b/a KOHLS.COM,
Defendant.

Case No.: 23-cv-01988-AJB-KSC

**ORDER GRANTING IN PART AND
DENYING IN PART DEFENDANT'S
MOTION TO DISMISS
(Doc. No. 4)**

17 Presently pending before the Court is Defendant Kohl's, Inc.'s motion to dismiss
18 Plaintiff Miguel Esparza's First Amended Class Action Complaint ("FAC") pursuant to
19 Federal Rule of Civil Procedure 12(b)(6). (Doc. No. 4.) Plaintiff filed an opposition to the
20 motion to dismiss, (Doc. No. 6), to which Defendant replied, (Doc. No. 7). Pursuant to
21 Civil Local Rule 7.1.d.1, the Court finds the instant matter suitable for determination on
22 the papers and without oral argument. For the reasons stated herein, the Court **GRANTS**
23 **IN PART AND DENIES IN PART** the motion to dismiss Plaintiff's FAC.

24 ///

25 ///

26 ///

27 ///

I. BACKGROUND¹

Plaintiff Miguel Esparza is a California resident who visited Defendant Kohl's, Inc.'s website and conducted a brief conversation with an agent of Defendant's through its website's chat feature. (FAC, Doc. No. 1-2, ¶ 3.) Plaintiff alleges Defendant allowed Ada Support Inc. ("ASI") "to embed its chat technology code into the chat feature offered on Defendant's website" in order to enable eavesdropping. (*Id.* ¶ 27.) The FAC further alleges these malware tools "secretly install[] a 'persistent cookie' on every user's device" and "de-anonymizes website visitors[.]" (*Id.*) After using Defendant's chat feature, Plaintiff contends "Defendant obtained plaintiff's personal information and embedded Plaintiff's identity into the malware companies' extensive 'gray market CAI' database, which the malware companies share virally with other companies that purchase their products." (*Id.* ¶ 21.) Plaintiff further asserts "Defendant also allows [ASI] to wiretap and eavesdrop upon class member communications through the website chat feature in violation of California law." (*Id.* ¶ 24.)

Plaintiff brings four claims under the California Invasion of Privacy Act, Cal. Pen. Code § 631(a); the California Computer Data Access and Fraud Act ("CDAFA"), Cal. Pen. Code § 502; the California Constitution for invasion of privacy; and for intrusion upon seclusion. Defendant moves to dismiss all three claims pursuant to Federal Rule of Civil Procedure 12(b)(6).

II. LEGAL STANDARD

A motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the pleadings and allows a court to dismiss a complaint upon a finding that the plaintiff has failed to state a claim upon which relief may be granted. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). The court may dismiss a complaint as a matter of law for: "(1) lack of cognizable legal theory or (2) insufficient facts under a cognizable legal claim." *SmileCare Dental*

¹ The facts incorporated herein are taken from Plaintiff's FAC and are construed as true for the limited purpose of resolving the instant motion. *See Brown v. Elec. Arts, Inc.*, 724 F.3d 1235, 1247 (9th Cir. 2013).

1 *Grp. v. Delta Dental Plan of Cal.*, 88 F.3d 780, 783 (9th Cir. 1996) (citation omitted).
2 However, a complaint survives a motion to dismiss if it contains “enough facts to state a
3 claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570
4 (2007).

5 Notwithstanding this deference, the reviewing court need not accept legal
6 conclusions as true. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). It is also improper for the
7 court to assume “the [plaintiff] can prove facts that [he or she] has not alleged”
8 *Associated Gen. Contractors of Cal., Inc. v. Cal. State Council of Carpenters*, 459 U.S.
9 519, 526 (1983). On the other hand, “[w]hen there are well-pleaded factual allegations, a
10 court should assume their veracity and then determine whether they plausibly give rise to
11 an entitlement to relief.” *Iqbal*, 556 U.S. at 679. The court only reviews the contents of the
12 complaint, accepting all factual allegations as true, and drawing all reasonable inferences
13 in favor of the nonmoving party. *Thompson v. Davis*, 295 F.3d 890, 895 (9th Cir. 2002).

14 **III. REQUESTS FOR JUDICIAL NOTICE**

15 While the scope of review on a motion to dismiss for failure to state a claim is limited
16 to the complaint, a court may consider evidence on which the complaint necessarily relies
17 if: “(1) the complaint refers to the document; (2) the document is central to the plaintiff[’s]
18 claim; and (3) no party questions the authenticity of the copy attached to the 12(b)(6)
19 motion.” *Daniels-Hall v. Nat’l Educ. Ass’n*, 629 F.3d 992, 998 (9th Cir. 2010) (internal
20 quotation marks and citations omitted). Furthermore, Federal Rule of Evidence 201 permits
21 judicial notice of a fact when it is “not subject to reasonable dispute because it: (1) is
22 generally known within the trial court’s territorial jurisdiction; or (2) can be accurately and
23 readily determined from sources whose accuracy cannot reasonably be questioned.” *Welk*
24 *v. Beam Suntory Imp. Co.*, 124 F. Supp. 3d 1039, 1041–42 (S.D. Cal. 2015).

25 **1. Request for Judicial Notice in Support of Defendant’s Motion to Dismiss**

26 As part of its motion to dismiss, Defendant requests the Court to take judicial notice
27 of the following exhibits in support of its Motion to Dismiss: (A) Kohl’s Privacy Policy,
28 effective on December 6, 2022; (B) Kohl’s Privacy Policy, effective on November 3, 2023;

1 (C) the court’s order in *Esparza v. Lenox Corporation*, No. 3:22-cv-09004 (N.D. Cal.),
2 dated May 24, 2023; (D) the court’s order in *Esparza v. UAG Escondido AI, Inc.*, No. 3:23-
3 cv-00102 (S.D. Cal.), dated July 27, 2023; (E) the court’s order in *Esparza v. Ecco USA,*
4 *Inc.*, No. 37-2023-00009235-CU-CR-CTL (San Diego Cnty.), dated July 31, 2023; and
5 (F) the court’s order in *Esparza v. ECI Software Solutions, Inc.*, No. 37-2023-00025427-
6 CU-CR-CTL (San Diego Cnty.), dated October 27, 2023. (Doc. No. 4-2 at 2.) Plaintiff
7 opposes the request for judicial notice as to Exhibits A and B. (Doc. No. 6 at 29.)

8 Regarding Exhibits A and B, there is a dispute as to the authenticity of these
9 documents, and they are not referred to in the complaint and are not central to Plaintiff’s
10 claim. Accordingly, the Court declines to take judicial notice of these documents.

11 As to Exhibits C through F, the Court may take judicial notice of court filings. *See*
12 *Rowland v. Paris Las Vegas*, No. 3:13-CV-02630-GPC-DHB, 2014 WL 769.93, at *2 (S.D.
13 Cal. Feb. 25, 2014) (citing *Reyn’s Pasta Bella, LLC v. Visa USA, Inc.*, 442 F.3d 741, 746
14 n.6 (9th Cir. 2006)). However, “[w]hile the authenticity and existence of a particular order,
15 motion, pleading or judicial proceeding, which is a matter of public record, is judicially
16 noticeable, veracity and validity of its contents . . . are not.” *United States v. S. Cal. Edison*
17 *Co.*, 300 F. Supp. 2d 964, 974 (E.D. Cal. 2004). Therefore, the Court **GRANTS**
18 Defendant’s requests for judicial notice of Exhibits C through F for the stated purpose that
19 these documents exist.

20 **2. Request for Judicial Notice in Support of Plaintiff’s Response in** 21 **Opposition to Motion to Dismiss**

22 In opposition to Defendant’s motion to dismiss, Plaintiff requests judicial notice of
23 eight separate orders and transcripts filed in various state and federal courts. (*See* Doc. No.
24 6-5 at 2.) As stated above, the Court may take judicial notice of court filings for the limited
25 purpose that these documents exist. *See Rowland*, 2014 WL 769.93, at *2; *S. Cal. Edison*
26 *Co.*, 300 F. Supp. 2d at 974. Therefore, the Court **GRANTS** Plaintiff’s requests for judicial
27 notice of Exhibits 1 through 8 for the stated purpose that these documents exist.

28 ///

1 **IV. DISCUSSION**

2 **A. Section 631(a) of CIPA**

3 Section 631 of the California Penal Code imposes liability on any person:

4 [1] who, by means of any machine, instrument, or contrivance, or in any other
5 manner, intentionally taps, or makes any unauthorized connection, whether
6 physically, electrically, acoustically, inductively, or otherwise, with any
7 telegraph or telephone wire, line, cable, or instrument, including the wire, line,
8 cable, or instrument of any internal telephonic communication system, or

9 [2] who willfully and without the consent of all parties to the communication,
10 or in any unauthorized manner, reads, or attempts to read, or to learn the
11 contents or meaning of any message, report, or communication while the same
12 is in transit or passing over any wire, line, or cable, or is being sent from, or
13 received at any place within this state; or

14 [3] who uses, or attempts to use, in any manner, or for any purpose, or to
15 communicate in any way, any information so obtained, or

16 [4] who aids, agrees with, employs, or conspires with any person or persons
17 to unlawfully do, or permit, or cause to be done any of the acts or things
18 mentioned above in this section[.]

19 Cal. Penal Code § 631(a) (numbering and formatting added for reference). Courts have
20 interpreted Section 631(a) to contain three operative clauses, which cover “three distinct
21 and mutually independent patterns of conduct: (1) intentional wiretapping, (2) willfully
22 attempting to learn the contents or meaning of a communication in transit over a wire, and
23 (3) attempting to use or communicate information obtained as a result of engaging in either
24 of the two previous activities.” *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1134 (E.D.
25 Cal. 2021) (quoting *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (1978)) (internal
26 quotation marks omitted). Additionally, “Section 631(a) further contains a fourth basis for
27 liability, for anyone ‘who aids, agrees with, employs, or conspires with any person or
28 persons to unlawfully do, or permit, or cause to be done any of the’ other three bases for
liability.” *Id.* (quoting Cal. Penal Code § 631(a)).

///

1 Here, Plaintiff alleges Defendant is directly liable under Clauses Two and Three,
2 and that under Clause Four, Defendant is vicariously liable for aiding and abetting ASI's
3 "eavesdropping." (FAC ¶¶ 47–48.)

4 **1. Clause Two of Section 631(a)**

5 **a. Consent**

6 Defendant argues Plaintiff consented to the recording of his web chats due to the
7 nature of the communication, i.e., written messaging. (Doc. No. 4 at 16.) Specifically,
8 Defendant asserts "[s]uch communications are, by their very nature, recorded. . . . Each
9 party to a chat communication necessarily records that party's own message in sending it
10 to the other party." (*Id.* (quoting *Licea v. Vitacost.com, Inc.*, No. 3:22-cv-01854, 2023 WL
11 5086893, at *3 (S.D. Cal. July 24, 2023)).)

12 Plaintiff meets his burden to plead lack of consent. The statute prohibits
13 eavesdropping "without consent of all parties to the communication." Cal. Penal Code
14 § 631(a). Plaintiff alleges neither he nor class members expressly or impliedly consented
15 to any of Defendant's actions when they used the Website to chat with a Kohl's customer
16 service representative. (FAC ¶ 49.) That is sufficient at this stage. *See Javier v. Assurance*
17 *IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022) (finding there
18 was no prior consent when the complaint pled that neither party to the communication
19 requested the plaintiff's "consent prior to his filling out the insurance questionnaire");
20 *D'Angelo v. Penny OpCo, LLC*, No. 23-cv-0981-BAS-DDL, 2023 WL 7006793, at *7
21 (S.D. Cal. Oct. 24, 2023) (finding absence of consent where the plaintiffs were not
22 informed of the chat recording or interception, nor gave their express or implied consent).
23 Accordingly, this element is satisfied.

24 **b. Party Exemption**

25 Defendant's next argument is based on the party exemption rule. Specifically,
26 Defendant asserts ASI acted simply as an extension of Defendant—as a recorder—and
27 therefore ASI is entitled to the party exemption. (Doc. No. 4 at 15; Doc. No. 7 at 4.)

28 ///

1 Under this rule, a party to a communication cannot be held liable under section
2 631(a) for eavesdropping on its own conversation. *See In re Facebook, Inc. Internet*
3 *Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (stating CIPA contains “an exemption
4 from liability for a person who is a ‘party’ to the communication”); *Warden v. Kahn*, 99
5 Cal. App. 3d 805, 811 (1979) (“[S]ection 631 . . . has been held to apply only to
6 eavesdropping by a third party and not to recording by a participant to a conversation.”);
7 *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 898 (N.D. Cal. 2023) (stating
8 “a party to a conversation can record it without the other party’s knowledge without
9 incurring Section 631 liability”). District courts in California are split on whether this
10 exemption extends to third parties, particularly, third-party software providers. *See Javier*,
11 649 F. Supp. 3d at 899–901 (discussing two lines of cases). Some courts hold that software
12 providers who embed code onto a party’s website do not fall within the party exemption.
13 *Id.* at 899 (citing cases); *Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 WL
14 5485330, at *2 (N.D. Cal. Oct. 23, 2019) (“[I]t cannot be that anyone who receives a direct
15 signal escapes liability by becoming a party to the communication. Someone who presses
16 up against a door to listen to a conversation is no less an eavesdropper just because the
17 sound waves from the next room reach his ears directly.”). Other courts hold these kinds
18 of software providers are simply extensions of the website owner, bringing them within the
19 party exemption. *Javier*, 649 F. Supp. 3d at 899 (citing cases); *Graham v. Noom, Inc.*, 533
20 F. Supp. 3d 823, 832–33 (N.D. Cal. Apr. 8, 2021) (reasoning that the tracking defendant
21 provided a tool, like a tape recorder, and therefore was not an eavesdropper).

22 In this case, Plaintiff pleads “ASI uses its record of Website users’ interaction with
23 Defendant’s chat feature to enable targeted marketing by Defendant and the Identity
24 Resolution Malware Companies[,]” thus asserting that ASI acted more than a mere
25 “recorder.” (FAC ¶ 33.) Moreover, Plaintiff argues the decisions extending the party
26 exemption to third parties “were wrongly decided” and urges the Court to disregard those
27 cases. (Doc. No. 6 at 15.) The Court finds here that whether ASI acts akin to a tape recorder
28 or whether its actions are closer to “an eavesdropper standing outside the door” is a

question of fact which is better answered after discovery. *See In re Facebook*, 956 F.3d at 607; *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021); *Kauffman v. Papa John's Int'l, Inc.*, No.: 22-cv-1492-L-MSB, 2024 WL 171363, at *7 (S.D. Cal. Jan. 12, 2024).

c. Content

Defendant further asserts Plaintiff's Section 631(a) claim under clause two should be dismissed because Plaintiff fails to allege the "contents" of any communication; specifically, that "Plaintiff has never provided any details of that 'conversation' he engaged in and has never asserted what the content of that communication was, and never claimed to have provided any confidential information during his 'brief' chat." (Doc. No. 4-1 at 20.) However, "there is no requirement that [a plaintiff] specifically allege the exact contents of [their] communications with [defendant]. Rather, [plaintiff] merely needs to show that the contents were not record information, such as [their] name and address." *Byars v. Goodyear Tire & Rubber Co.*, 654 F. Supp. 3d 1020, 1027 (C.D. Cal. 2023).

For purposes of Section 631(a)'s second clause, Plaintiff must allege that Defendant or ASI "read, or attempts to read, or to learn the contents or meaning of any message, report, or communication." Cal. Pen. Code § 631(a). Courts analyzing CIPA claims apply the same definitions for the federal Wiretap Act (18 U.S.C. §§ 2510–2523) where appropriate. *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 517 (C.D. Cal. 2021). "The Ninth Circuit has held that the 'contents' of an online communication under federal wiretap law 'refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication.'" *Yoon*, 549 F. Supp. 3d at 1082 (quoting *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014)).

Here, Plaintiff asserts in the FAC that "whenever a consumer chats via Defendant's Website, the chat is routed through ASI's servers so they may simultaneously collect a transcript of that chat, along with other user data, in real time and save it for later access." (FAC ¶ 27.)

1 Taking these allegations as true, Plaintiff has sufficiently alleged facts plausibly
2 showing Defendant recorded Plaintiff’s content communications with Defendant by
3 recording, among other things, a transcript of Plaintiff’s interactions with Defendant’s
4 website. *See Saleh*, 562 F. Supp. 3d at 517–18; *Kauffman*, 2024 WL 171363, at *9. For the
5 above reasons, Plaintiff’s FAC is sufficient to state a cause of action under the second
6 clause of Section 631(a) and the Court denies Defendant’s motion to dismiss on this
7 ground.

8 **d. The “In Transit” Requirement**

9 Liability under Clause Two arises when the purported CIPA violator “reads, or
10 attempts to read, a communication that is ‘in transit or passing over any wire, line, or cable,
11 or is being sent from, or received at any place within’ California.” *Mastel*, 549 F. Supp. 3d
12 at 1135 (quoting Cal. Penal Code § 631(a)). Some courts have held that, at the motion to
13 dismiss stage, a plaintiff is not expected to prove or even know how and when its
14 communications were captured. *D’Angelo*, 2023 WL 7006793, at *8; *see, e.g., In re Vizio*,
15 *Inc. Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1228 (C.D. Cal. 2017). “Indeed, a
16 pleading standard to the contrary would require the CIPA plaintiff to engage in a one-sided
17 guessing game because the relevant information about data capture typically resides
18 uniquely in the custody and control of the CIPA defendant and its third-party recorder.”
19 *D’Angelo*, 2023 WL 7006793, at *8. Still, a CIPA plaintiff “must provide fair notice to
20 [d]efendant[]” of how and when he “believe[s]” the defendant or the conspiring third party
21 intercepts his communications. *In re Vizio*, 238 F. Supp. 3d at 1228; *see also Licea v.*
22 *American Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072, 1085 (C.D. Cal. 2023) (“Plaintiffs
23 must provide more than conclusory allegations that messages were intercepted ‘during
24 transmission in real time.’”).

25 Plaintiff successfully pleads that ASI intercepted Plaintiff’s chat with Defendant.
26 Plaintiff alleges the Kohl’s Website chat feature operates through ASI’s servers, allowing
27 real-time interception of the communication. (FAC ¶ 28 (“ASI acquires Website visitors’
28 chat communications by first having its software route them to ASI’s own computer servers

1 that it owns, control, and maintains. The secret code enables and allows ASI to secretly
2 intercept in real time, eavesdrop upon, and store transcripts of consumers’ chat
3 communications”).) Defendant’s argument that Plaintiff does not allege “the timing
4 of the alleged ‘interception’ of the communication” thus necessarily fails. (Doc. No. 4-1 at
5 22.)

6 Ultimately, Plaintiff plausibly pleads that Defendant has violated CIPA Clause Two
7 in allowing ASI to “listen in” on chats between Website users and Kohl’s customer service
8 representatives.

9 **2. Clause Three of Section 631(a)**

10 Clause Three creates liability under CIPA for any party “who uses, or attempts to
11 use, in any manner, or for any purpose, or to communicate in any way, any information [as
12 laid out in Clauses One and Two].” Cal. Penal Code § 631(a). However, unlike Clause
13 Two, Clause Three specifically includes a use requirement.

14 Here, Plaintiff alleges ASI intercepts chat transcripts and provides them to Meta and
15 third-party identity resolution malware companies, resulting in Website visitors being
16 bombarded with targeted advertising, emails, and telephone calls. (FAC ¶ 31.) Moreover,
17 “ASI uses its record of Website users’ interaction with Defendant’s chat feature to enable
18 targeted marketing by Defendant and the Identity Resolution Malware Companies.” (*Id.*
19 ¶ 33.) He further alleges that Defendant and ASI “profit from secretly exploiting their
20 ability to identify anonymous individuals who have visited Defendant’s website.” (*Id.*
21 ¶ 34.) These allegations lead to a plausible inference that ASI is using the information it
22 gathers in some manner for Kohl’s and its own benefit. *See Valenzuela v. Nationwide Mut.*
23 *Ins. Co.*, No.: 2:22-cv-06177-MEMF-SK, 2023 WL 5266033, at *6 (C.D. Cal. Aug. 14,
24 2023). Accordingly, Plaintiff has stated a violation of the third clause by ASI. *See* Cal.
25 Penal Code § 631(a).²

26
27
28 ² Section 631 imposes liability on anyone who aids another in violating any of the three main clauses. *See*
Cal. Penal Code § 631(a). Although Defendant asserts in its Motion to Dismiss that Plaintiff has not

1 **B. CDAFA**

2 Under CDAFA, a person who knowingly accesses a computer system or computer
3 data may be guilty of a public offense. Section 502(c) states in relevant part:

4 [A]ny person who commits any of the following acts is guilty of a public
5 offense:

6 (1) Knowingly accesses and without permission . . . uses any data, computer,
7 computer system, or computer network in order to . . . wrongfully control or
8 obtain money, property, or data.

9 (2) Knowingly accesses and without permission takes, copies, or makes use
10 of any data from a computer, computer system, or computer network, or takes
11 or copies any supporting documentation, whether existing or residing internal
or external to a computer, computer system, or computer network.

12 Cal. Penal Code § 502(c)(1)–(2). “With the exception of § 502(c)(8), all of the prohibited
13 conduct articulated in § 502(c) requires that the defendant act ‘without permission’”
14 *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1098 (N.D. Cal. 2015). To bring a claim under
15 the statute, the owner of the data must also adequately allege that “damage or loss by reason
16 of a violation” of the statute was suffered. Cal. Penal Code § 502(e)(1).

17 Plaintiff contends in the FAC that Defendant violated CDAFA by “knowingly
18 installing the Identity Resolution Malware to access class member devices and extract their
19 personal information” (FAC ¶ 55.) Plaintiff argues this Identity Resolution Malware
20 secretly installs cookies on each user’s device and de-anonymizes users by connecting
21 touch points, such as emails, devices, and purchases. (*Id.* ¶ 20.)

22 Defendant asserts the FAC fails to allege a breach of sections 501(c)(1) and (2)
23 because Plaintiff does not allege that *his* device, either smartphone or computer, had
24

25 _____
26
27 sufficiently alleged aiding-and-abetting liability against it, it does not make any argument that it did not
28 aid, permit, or cause ASI’s violations. (*See generally* Doc. No. 4.) Thus, the Court **DENIES** Defendant’s
motion to dismiss as to whether Kohl’s is liable for ASI’s alleged violations.

1 technical or code-based barriers breached during his interaction with the Website. (Doc.
2 No. 4-1 at 24.) Moreover, Defendant argues Plaintiff does not plead any cognizable
3 “damage or loss” as required under CDAFA.

4 **1. “Without Permission”**

5 First, Defendant asserts a website’s access to an IP address is not “data” because an
6 IP address is not located on a device itself, but rather, an address assigned by the user’s
7 Internet Service Provider. (Doc. No. 4-1 at 24.) Thus, asserts Defendant, Plaintiff cannot
8 allege his device had technical or code-based barriers breached, which is required by
9 Section 502’s “without permission” element. (*Id.*)

10 In opposition, Plaintiff argues that *technical circumvention* to access Plaintiff’s
11 computer is not necessary to satisfy the “without permission” element of Section 502. (Doc.
12 No. 6 at 31 (citing *Greenley v. Kochava, Inc.*, No. 22-CV-01327-BAS-AHG, 2023 WL
13 4833466 (S.D. Cal. July 27, 2023).) Plaintiff requests the Court to follow *Greenley*, which
14 held “the phrase ‘without permission’ is not limited to conduct that circumvents a device
15 barrier or ‘hacks’ a computer system.” *Greenley*, 2023 WL 4833466, at *14; *see In re*
16 *Carrier IQ*, 78 F. Supp. 3d at 1099 (“Nothing in the [*Facebook, Inc. v.*] *Power Ventures*[,
17 No. C08-05780 JW, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010)] decision held
18 that overcoming ‘technical or code-based barriers’ designed to prevent access was the only
19 way to establish that the Defendant acted without permission.”). Defendant replies that
20 Plaintiff’s reliance on *Greenley*, is misplaced because there, the defendant was alleged to
21 have surreptitiously circumvented barriers which plaintiffs relied upon to protect their data,
22 which is not the case here. (Doc. No. 7 at 9.)

23 The Court follows the broadened interpretation of “without permission” and finds
24 “the phrase ‘without permission’ is not limited to conduct that circumvents a device barrier
25 or ‘hacks’ a computer system.” *Greenley*, 2023 WL 4833466, at *14. Moreover, Defendant
26 cites no case in which access to an IP address would not constitute “data” under CDAFA.
27 As such, Defendant’s motion to dismiss on this basis fails.

28 ///

2. Damage or Loss

Second, Defendant argues Plaintiff fails to allege he suffered any cognizable “damage or loss” from the alleged hack. (Doc. No. 4-1 at 25–26.) In response, Plaintiff states “the Court can and should infer that the FAC alleges that Defendant unfairly profited from ‘secretly exploiting their ability to identify anonymous individuals who have visited Defendant’s website.’” (Doc. No. 6 at 32 (quoting FAC ¶ 34).)

To bring a private civil cause of action under section 502, which is otherwise a criminal statute, a plaintiff must plead that he “suffers damage or loss” due to the criminal violation. Cal. Penal Code § 502(e).

Here, Plaintiff sufficiently alleges Defendant has a stake in the value of his misappropriated data. In the FAC, Plaintiff explains how Defendant and ASI “all profit from secretly exploiting their ability to identify anonymous individuals who have visited Defendant’s website” and that ASI “uses its record of Website users’ interaction with Defendant’s chat feature to enable targeted marketing by Defendant and the Identity Resolution Malware Companies.” (FAC ¶¶ 33, 35.) In *In re Facebook*, the Ninth Circuit found that plaintiffs had sufficiently alleged their browsing histories carried financial value. 956 F.3d at 600. Similarly here, Plaintiff alleges there is a market for his data that Defendant and ASI allegedly profit from. “The Ninth Circuit’s decision stands for the proposition that plaintiffs can state an economic injury for their misappropriated data.” *Brown v. Google LLC*, No.: 4:20-cv-3664-YGR, 2023 WL 5029899, at *19 (N.D. Cal. Aug. 7, 2023).

As such, the Court **DENIES** Defendant’s motion to dismiss Plaintiff’s CDAFA claim.

C. Invasion of Privacy and Intrusion Upon Seclusion

By way of his third cause of action, Plaintiff alleges the disclosure of his personal information and browsing history constitutes a violation of his right to privacy pursuant to Article I, Section 1 of the California Constitution. (FAC ¶¶ 56–65.) Similarly, Plaintiff’s fourth cause of action alleges that the secret access of Plaintiff’s device, mining of his

1 personal data, and sharing the data with malware companies constitutes an intrusion upon
2 seclusion. (*Id.* ¶¶ 66–72.) Defendant asserts Plaintiff’s claims fail because he cannot allege
3 facts showing that (1) his computer/smart phone was “accessed” by Defendant, or
4 (2) “malware” was installed on his device. (Doc. No. 4-1 at 27.) Defendant further asserts
5 that Plaintiff cannot meet the “high bar” of showing that any alleged intrusion was “highly
6 offensive.” (*Id.*)

7 “To state a claim for intrusion upon seclusion under California common law, a
8 plaintiff must plead that (1) a defendant ‘intentionally intrude[d] into a place, conversation,
9 or matter as to which the plaintiff has a reasonable expectation of privacy [,]’ and (2) that
10 the intrusion ‘occur[red] in a manner highly offensive to a reasonable person.’” *In re*
11 *Facebook*, 956 F.3d at 601 (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286
12 (2009)). “A claim for invasion of privacy under the California Constitution involves similar
13 elements.” *Id.* Plaintiffs must plead “that (1) they possess a legally protected privacy
14 interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is ‘so
15 serious . . . as to constitute an egregious breach of the social norms’ such that the breach is
16 ‘highly offensive.’” *Id.* (quoting *Hernandez*, 47 Cal. 4th at 287). “Because of the similarity
17 of the tests, courts consider the claims together and ask whether: (1) there exist a reasonable
18 expectation of privacy, and (2) the intrusion was highly offensive.” *Id.* Whether the conduct
19 was highly offensive can rarely be resolved at the pleading stage. *Id.* at 606.

20 As the California Supreme Court has explained, “the plaintiff in an invasion of
21 privacy case must have conducted himself or herself in a manner consistent with an actual
22 expectation of privacy” *Hill v. Nat’l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 26 (1994);
23 *see, e.g., Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (1979). “Courts have been hesitant to
24 extend the tort of invasion of privacy to the routine collection of personally identifiable
25 information as part of electronic communications.” *In re Vizio*, 238 F. Supp. 3d at 1233.
26 “By contrast, collection of intimate or sensitive personally identifiable information may
27 amount to a highly offensive intrusion.” *Id.* “Further, more routine data collection practices
28 may be highly offensive if a defendant disregards consumers’ privacy choices while

1 simultaneously ‘h[olding] itself out as respecting them.’” *Id.* (quoting *In re Nickelodeon*
2 *Consumer Privacy Litig.*, 827 F.3d 262, 292 (3d Cir. 2016)).

3 Here, the FAC does not plead any facts to suggest Defendant collected intimate or
4 sensitive personally identifiable information or otherwise disregarded Plaintiff’s privacy
5 choices while simultaneously holding itself out as respecting them. *See id.* The fact that
6 ASI’s software allegedly captured, among other things, Plaintiff’s “personal details” and
7 “browsing history,” (FAC ¶ 59), and IP address, (Doc. No. 6 at 32–33), is insufficient to
8 demonstrate that Defendant’s conduct constituted a serious invasion of a protected privacy
9 interest. *See Hill*, 7 Cal. 4th at 26; *In re Vizio*, 238 F. Supp. 3d at 1233; *Saleh*, 562 F. Supp.
10 3d at 525; *Brown*, 2023 WL 5029899, at *20 (“Although Ninth Circuit law indicates that
11 users may not have a reasonable expectation of privacy over the IP addresses of the
12 websites they visit or URLs that only reveal basic identification information, they do over
13 URLs that disclose either unique ‘search terms’ or the ‘particular document within a
14 website that a person views.’”) (quoting *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069,
15 1088 (N.D. Cal. 2022)); *see also Yoon*, 549 F. Supp. 3d at 1086; *In re Google RTB*
16 *Consumer Privacy Litig.*, 606 F. Supp. 3d 935, 946–47 (N.D. Cal. 2022) (denying motion
17 to dismiss privacy claim and stating the “nature and volume of the collected information is
18 also important” where Google “sold sensitive personal information such as plaintiff’s IP
19 address, geo-location data, and web-browsing information, search terms, and sensitive
20 websites that plaintiffs visited relating to race, religion, sexual orientation, and health.”).

21 Accordingly, the Court **GRANTS** Defendant’s motion on Plaintiff’s claims for
22 invasion of privacy and intrusion upon seclusion, with leave to amend.

23 ///

24 ///

25 ///

26 ///

27 ///


28 ///

1 **V. CONCLUSION**

2 Based on the foregoing, the Court **GRANTS IN PART AND DENIES IN PART**
3 Defendant's motion to dismiss. Should Plaintiff desire to amend his complaint, he must
4 file a second amended complaint no later than April 5, 2024. Defendant must file a
5 responsive pleading no later than April 19, 2024.

6
7 **IT IS SO ORDERED.**

8
9 Dated: March 18, 2024

10 
11 Hon. Anthony J. Battaglia
12 United States District Judge
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28