UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION

CASE NO. 25-80458-CIV-CANNON/Reinhart

KRISTIN COBBS, LYNNE KAWAMINAMI, and **LORETTA SCHWEINSBURG,**
individually and on behalf of all others similarly situated,

Plaintiffs,

v.

PETMED EXPRESS, INC.,

Defendant.
_____/

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

THIS CAUSE comes before the Court upon Defendant PetMed Express, Inc.'s Motion to Dismiss Plaintiffs' First Amended Complaint under Rule 12(b)(1) and Rule 12(b)(6) (the "Motion") [ECF No. 23]. The Court has reviewed the Motion, Plaintiffs' Opposition [ECF No. 34], Defendant's Reply [ECF No. 35], Plaintiffs' Sur-reply [ECF No. 40], the First Amended Complaint [ECF No. 21], attachments to the Motion properly considered under the incorporation by reference doctrine, and the Notices of Supplemental Authority [ECF Nos. 56–57].[1] Fully advised in the premises, the Motion is **GRANTED IN PART AND DENIED IN**

[1] The attachments consist of Defendant's Privacy Policy [ECF No. 23-1], Meta's Terms of Service [ECF No. 23-2], and Meta's Privacy Policy [ECF No. 23-3]. Although Plaintiff characterizes these materials as improperly submitted [*see* ECF No. 34 p. 15], all three are explicitly referenced and quoted in the First Amendment Complaint (with two even hyperlinked in the pleading itself) [ECF No. 21 pp. 19–20]; they each concern the central question whether Plaintiffs consented to the alleged interceptions at issue; and nowhere do Plaintiffs dispute their authenticity. *See Johnson v. City of Atlanta*, 107 F.4th 1292, 1300 (11th Cir. 2024) (authorizing incorporation by reference of undisputedly authentic exhibits central to a plaintiff's claims).

PART as indicated below.

RELEVANT BACKGROUND AND PROCEDURAL HISTORY[2]

In April 2025, Plaintiffs Cobbs, Kawaminami, and Schweinsburg, individually and on behalf of two putative classes, filed suit against Defendant PetMed Express, Inc., alleging violations of the Federal Wiretap Act ("Electronic Communications Privacy Act" or "ECPA"), 18 U.S.C. § 2511(1)(a); the California Invasion of Privacy Act ("CIPA"), *see* Cal. Penal Code §§ 631–632; the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and common law intrusion upon seclusion [ECF No. 1 pp. 35–42]. After Defendant moved to dismiss Plaintiffs' claims [ECF No. 20], Plaintiffs filed the operative First Amended Complaint [ECF No. 21]. Defendant thereafter brought the instant Motion to Dismiss, seeking to dispose of all counts for lack of Article III standing and for failure to state a claim [ECF No. 23].

Defendant PetMed owns and operates www.1800petmeds.com, one of the largest online pharmacies for veterinary prescriptions [ECF No. 21 ¶ 1]. Plaintiffs are customers or potential customers of Defendants, who allege that they visited Defendant's website to browse for veterinary medicine [ECF No. 21 ¶¶ 7–9]. While doing so, Plaintiffs allege that Defendant assisted various third parties—like Meta, Attentive, and Zeta—with intercepting Plaintiffs' communications containing confidential veterinary information and personally identifiable information [ECF No. 21 ¶¶ 7–9]. This assistance, Plaintiffs say, was made possible because Defendant integrated third party technology on its website such as the Meta Pixel, which "surreptitiously directs the user's browser to send a separate message to Meta's servers" containing things users have added

[2] The following allegations are drawn from Plaintiffs' First Amended Complaint and accepted as true for purposes of this Order.

to their cart, their browsing choices, links clicked, search queries, and form-inputs [*see, e.g.*, ECF No. 21 ¶¶ 42–64]. Meta then processes that information, analyzes it, and assimilates it into datasets and individual profiles that allow Meta to more effectively target consumers [ECF No. 21 ¶¶ 43–44; *see also* ECF No. 21 ¶¶ 82–84, 97–102 (similar allegations against Attentive and Zeta)]. Once this information is processed by Meta and similar third parties, Plaintiffs allege that Defendant knowingly uses the intercepted communications to build "Custom Audiences" and run targeted advertisements on its website [*see, e.g.*, ECF No. 21 ¶ 63]. Yet, according to Plaintiffs, at no point throughout this process does Defendant "put consumers on notice" of the third-party browser-tracking software implemented in its website [ECF No. 21 ¶ 65]. Instead, Defendant expressly warrants in its privacy policy that it "follow[s] generally accepted industry practices to make sure [personal information] is not inappropriately misused, accessed, disclosed, altered or destroyed" [*see* ECF No. 21 ¶ 65; ECF No. 23-1 p. 5].

As a remedy against Defendant's allegedly unlawful data-collection practices, Plaintiffs say they are entitled to statutory damages under the Electronic Communications Privacy Act and various California privacy statutes cited above, along with damages for common law intrusion upon seclusion [ECF No. 21 pp. 37–46].

LEGAL STANDARDS

Federal Rule of Civil Procedure 12(b)(1)

Challenges to a party's standing are properly raised under Federal Rule of Civil Procedure 12(b)(1) as a jurisdictional challenge to a court's subject matter jurisdiction. *Stalley ex rel. U.S. v. Orlando Reg'l Healthcare Sys., Inc.*, 524 F.3d 1229, 1232 (11th Cir. 2008). A facial attack on a plaintiff's standing challenges whether the plaintiff "sufficiently alleged a basis of subject matter jurisdiction," applying the standards similar to those governing 12(b)(6) review. *Houston v.*

Marod Supermarkets, Inc., 733 F.3d 1323, 1335 (11th Cir. 2013). The Court must merely "look and see if the plaintiff has sufficiently alleged a basis of subject matter jurisdiction, and the allegations in [the] complaint are taken as true for the purposes of the motion." *Lawrence v. Dunbar*, 919 F.2d 1525, 1529 (11th Cir. 1990) (alteration adopted) (quotation omitted).

Federal Rule of Civil Procedure 12(b)(6)

Rule 8(a)(2) requires complaints to provide "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). To avoid dismissal under Rule 12(b)(6), a complaint must allege facts that, if accepted as true, "state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *see* Fed. R. Civ. P. 12(b)(6). A claim for relief is plausible if the complaint contains factual allegations that allow "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). "[C]onclusory allegations, unwarranted deductions of facts, or legal conclusions masquerading as facts will not prevent dismissal." *Oxford Asset Mgmt., Ltd. v. Jaharis*, 297 F.3d 1182, 1188 (11th Cir. 2002).

DISCUSSION

Defendant moves for dismissal of all claims in Plaintiffs' First Amended Complaint pursuant to Rules 12(b)(1) and 12(b)(6) [ECF No. 23 pp. 3–6]. As to jurisdiction, Defendant argues that Plaintiffs have not alleged a concrete injury sufficient to confer Article III standing [ECF No. 23 p. 3; ECF No. 35 pp. 1–2]. On the merits, Defendant raises a host of arguments challenging the individual claims, including that it did not "intercept" Plaintiffs' communications as required to establish liability under the ECPA, 18 U.S.C. §§ 2511(1)(a), 2511(4); that Defendant did not acquire the "contents" of Plaintiffs' communications, as necessary to trigger liability under CIPA's wiretap provision, *see* Cal. Penal Code § 631; that none of the communications between

the parties were confidential within the meaning of CIPA's eavesdropping provision, *see* Cal. Penal Code § 632; that Defendant lacked a tortious intent for purposes of the crime-tort exception in the ECPA, *see* 18 U.S.C. § 2511(2)(d); that Plaintiffs suffered no cognizable loss under the CDAFA, *see* Cal. Penal Code § 502; that Plaintiffs consented to the transmission of their data; and that any alleged intrusion was not purposeful or highly offensive under the common law tort of intrusion upon seclusion [ECF No. 23]. Plaintiffs dispute all of these arguments, explaining that they have alleged standing because Defendant intruded into their sensitive and confidential communications; that Defendant "intercepted" their communications for a tortious purpose under the ECPA; that Defendant facilitated the third parties' acquisition of the "contents" of Plaintiffs' communications by ascertaining the precise files requested by Plaintiffs through search queries, full-string URLs (uniform resource locator for web pages), and the text of buttons clicked under the CIPA; that their data has inherent value and thus that they suffered a cognizable loss under the CDAFA; and that the intrusion into their data was purposeful and highly offensive for purposes of common law intrusion upon seclusion [ECF No. 34]. The Court addresses these arguments in turn.

I. Plaintiffs have Article III standing to bring the claims alleged.

Defendant's threshold submission is that Plaintiffs lack Article III standing to sue because they have not explained how they were injured, financially or otherwise, from the third parties' alleged acquisition of their data [ECF No. 23 p. 3]. This is a facial attack on Plaintiffs' standing, *see Lawrence*, 919 F.2d at 1529, and it rests on the notion that Plaintiffs' allegations in the First Amended Complaint, accepted as true, amount to a bare statutory violation that does not, by itself, establish a concrete injury-in-fact following *TransUnion LLC v. Ramirez*, 594 U.S. 413, 427 (2021), and related authorities [ECF No. 23 pp. 3–5; ECF No. 35 pp. 1–2].

The "irreducible constitutional minimum of standing" itself has three components—injury-in-fact, causation, and redressability—only the first of which is in dispute here [*see* ECF No. 23 p. 3]. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). To allege a sufficient injury-in-fact for Article III purposes, a plaintiff must have a "personal stake" in the litigation and must allege a "concrete and particularized" *de facto* harm that is "real, and not abstract." *Raines v. Byrd*, 521 U.S. 811, 819 (1997); *TransUnion LLC*, 594 U.S. at 427 (quotation omitted). The injury-in-fact can be "tangible," such as "physical injury or financial loss," or it may be "intangible," such as a concrete harm resulting from a statutory violation or a substantial risk of future harm that is "certainly impending" and supported by evidence. *See Nelson v. Experian Info. Sols. Inc.*, 144 F.4th 1350, 1353, 1356 (11th Cir. 2025).

When a plaintiff asserts an "intangible" harm resulting from a statutory violation, the court must conduct an independent injury-in-fact evaluation, "assess[ing] 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." *TransUnion LLC*, 594 U.S. at 424 (quoting *Spokeo v. Robins*, 578 U.S. 330, 341 (2016)). The *TransUnion* Court provided three such examples of intangible harms with historical analogues: "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.* at 425. While a statute that matches up with one of those torts is sufficient to provide Article III standing, a bare statutory violation that does not have a historical basis for its injury, the Court explained, is not. *Id.* at 440.

Getting closer to the present case, the Eleventh Circuit has addressed Article III standing in the context of transmission of private user data to a third party and applied the historical analogue test for intangible harm—ultimately finding an injury-in-fact sufficient to confer Article III standing in analogous circumstances. Specifically, in *Perry v. Cable News Network, Inc.*, 854

F.3d 1336 (11th Cir. 2017), a smartphone user brought a class action against a network, alleging a violation of the Video Privacy Protection Act after the smartphone user's viewing activity on the network's app was disclosed by the network to a third-party data analytics company.[3] *Id.* at 1338–39. That type of invasion of privacy harm, the Eleventh Circuit determined, matched up with the longstanding common law tort of intrusion upon seclusion and ultimately was sufficient to confer standing based on the wrongful disclosure of personal information—without proof of additional harm. *Id.* at 1340–41. A corollary to this principle, drawing from the Eleventh Circuit's en banc decision in *Drazen v. Pinto*, 74 F.4th 1336 (11th Cir. 2023), is that a plaintiff whose Article III standing is analogized to the common law tort of intrusion upon seclusion need not establish that the intrusion is "highly offensive" to a reasonable person, *id.* at 1343–44—because, again, what matters for standing purposes is whether the harm alleged shares "a 'close relationship'" to the historical tort "in *kind*, not *degree*."[4] *Id.* (emphasis added) (quoting *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.)); *see Drazen*, 74 F.4th at 1345 (holding that consumers who received single unwanted, illegal telemarketing text message from web-hosting company suffered a concrete injury-in-fact, as required to have standing).

[3] Although *Perry* was decided before *TransUnion*, *Perry* followed the Court's direction in *Spokeo* to analyze the relationship between the alleged harm and a traditional American tort and did so by matching the harm to the specific elements of intrusion upon seclusion. *See* 854 F.3d at 1340–41 (citing *Spokeo*, 578 U.S. at 340–42). Later in *TransUnion*, the "Supreme Court . . . ratified [that] approach." *Hunstein*, 48 F.4th at 1239; *see also Davis v. Pro. Parking Mgmt. Corp.*, No. 22-14026, 2023 WL 4542690, at *3 (11th Cir. July 14, 2023) ("*Perry* properly followed this Circuit's and the Supreme Court's precedent by inquiring into whether a statutory violation had a common-law analogue and likening the Video Privacy Protection Act . . . to invasion of privacy.").

[4] The Restatement defines intrusion upon seclusion as follows: "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B.

Applying these standards here, Plaintiffs' allegations of harm, accepted as true, are sufficient to establish a concrete injury-in-fact. Plaintiffs allege that Defendant, by knowingly installing third-party tracker software on its website, caused the disclosure to third parties of Plaintiffs' confidential data transmitted via Defendant's website, such as Plaintiffs' "form inputs," search queries, content-based URL's, and button clicks [*see, e.g.*, ECF No. 21 ¶¶ 7–9, 48, 52, 92, 102, 133, 135, 148, 156–57, 161, 170].[5] These allegations are analogous to the facts deemed sufficient in *Perry*, where the plaintiff-class alleged that the defendant "track[ed] the user's views of news articles and videos," "collect[ed] a record of th[at] viewing activity," and "sen[t] the collected record to . . . a third party company that conducts data analytics." 854 F.3d at 1339. No more is required for Article III purposes under *Perry* or *Drazen*. Nor, as Defendant suggests, are Plaintiffs obligated to plead an independent injury on top of the disclosure of their data; to quantify the value of such data; or to plead a "highly offensive" form of injury [ECF No. 23 pp. 3–6; ECF No. 35 pp. 1–2]. *See Perry*, 854. F3d at 1341 ("[I]n the tort of intrusion upon seclusion, 'the *intrusion itself* makes the defendant subject to liability, even though there is no publication or other use,' meaning a showing of additional harm is not necessary to create liability." (alteration adopted) (quoting Restatement (Second) of Torts § 652B cmt. b)); *Drazen*, 74 F.4th at 1343–44 (rejecting the common law requirement that the intrusion upon seclusion be "highly offensive").[6]

---

[5] Although standing "is not dispensed in gross," *Town of Chester, N.Y. v. Laroe Ests., Inc.*, 581 U.S. 433, 439 (2017) (quotation omitted), it is appropriate in this case to examine standing holistically as to all of the related privacy claims because Plaintiffs' asserted privacy invasion is the same throughout. *See, e.g.*, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598–99 (9th Cir. 2020) (assessing standing for related privacy claims together); *In re BPS Direct, LLC*, 705 F. Supp. 3d 333, 353 (E.D. Pa. 2023) (same). There is a separate statutory standing question as to Plaintiff's claim under the CDAFA, which is addressed below as a merits question. *See* Cal. Penal Code § 502(e)(1) (requiring owner of data to "suffer[] damage or loss"). *See infra* pp. 18–20.

[6] To the extent Defendant "believe[s] that the alleged conduct implicates privacy interests that are not legally protected, th[at] is an issue of the merits rather than of standing." *In re Google Inc.*

For these reasons, Plaintiffs have sufficiently alleged that they have suffered an injury-in-fact sufficient to confer Article III standing for all five of their claims. The Court now proceeds to analyze each of Plaintiffs' claims on the merits.

II. Plaintiffs state a plausible claim for relief under the ECPA (Count I).

Plaintiffs' first claim is brought under the ECPA. 18 U.S.C. §§ 2511(1)(a). The ECPA creates civil liability against any defendant who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." *See* 18 U.S.C. §§ 2511(1)(a), 2520(a). Plaintiffs argue that Defendant violated the ECPA by "closely assisting" the third parties in obtaining their personal information through the embedded third-party website software, thus "intentionally caus[ing] the third parties . . . to intercept [Plaintiffs'] electronic communications" [ECF No. 21 ¶¶ 133, 135].

Defendant makes two arguments for dismissal of Plaintiffs' ECPA claim. First, Defendant argues that the communications from the Plaintiffs' browsers to Defendant (and ultimately, to the third parties) were not "intercepted" within the meaning of the ECPA [*see* ECF No. 23 pp. 6–7]. Second, Defendant argues that, even if an interception occurred, it was lawful because Defendant was itself a party to the communications [*see* ECF No. 23 pp. 6–7]. Neither argument warrants dismissal under Rule 12(b)(6).

First, as to interception, the ECPA defines the term "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Although the Eleventh Circuit has not directly addressed the technology at issue here, the court acknowledged in *United States v.*

Cookie Placement Cons. Priv. Litig., 806 F.3d 125, 135 (3d Cir. 2015). Additionally, nothing in Defendant's briefing justifies a deviation from *Perry*, which rejected a standing challenge based on analogous tracking, collection, and disclosure of personal data. 854 F.3d at 1339.

Steiger, 318 F. 3d 1039 (11th Cir. 2003), albeit in dicta, that "some type of automatic routing software" that is used to "duplicate" and automatically forward a "message" likely would qualify as a contemporaneous interception under the ECPA. *Id.* at 1048–50 (rejecting claim of contemporaneous interception where third party accessed saved information on defendant's computer but suggesting that interception would exist in the case of automatic routing software used to send emails).[7] Plaintiffs' allegations—that their personal information is "intercepted" when it is instantly re-routed to the third parties' servers—are sufficiently analogous to the hypothetical email software deemed in *Steiger* to constitute a contemporaneous interception within the meaning of the ECPA. 318 F. 3d at 1048–50. Specifically, Plaintiffs allege that:

> [W]hen consumers access and navigate 1800.petmeds.com, Attentive's software script surreptitiously directs the user's browser to send a separate message to Attentive's server. This second, secret transmission contains the original GET request sent to the host website along with additional data that Attentive's code is configured to collect. This transmission is initiated by Attentive's code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's website—Defendant's own code, and Attentive's embedded code.

[*see* ECF No. 21 ¶ 88; *see also* ECF No. 21 ¶¶ 42–43, 101 (alleging the same process for Meta and Zeta)]. Based on those allegations—and consistent with the broad terms of the definition of "intercept" in the ECPA, *see* 18 U.S.C. § 2510(4) (defining "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any

[7] *See also Luis v. Zang*, 833 F.3d 619, 630 (6th Cir. 2016) (permitting ECPA claim to proceed at the 12(b)(6) stage, where plaintiff alleged that software "immediately and instantaneously" copied and sent electronic communications to a third party, which allowed for "near real-time monitoring" of plaintiff's emails); *United States v. Szymuszkiewicz*, 622 F.3d 701, 703 (7th Cir. 2010) (holding that an email system that automatically forwarded emails to the defendant within a second of the emails' arrival to the person's inbox qualified as an interception under the ECPA); *Zaratzian v. Abadir*, No. 10 CV 9049, 2014 WL 4467919, at *6 (S.D.N.Y. Sept. 2, 2014), *aff'd*, 694 F. App'x 822 (2d Cir. 2017) (holding at the summary judgment stage that the auto-forwarding of emails from plaintiff's email account to defendant's email account satisfied the contemporaneous standard for liability under the narrow "interception" standard applied to the ECPA).

electronic, mechanical, or other device")—the Court is satisfied that Defendant's "surreptitious," instant "separate message[s]" to the third parties (using data-capturing electronic tools) are close enough to the Eleventh Circuit's premonition of "some type of automatic routing software" for Plaintiffs to at least plausibly establish that Defendant contemporaneously intercepted their electronic communications under the ECPA. *Steiger*, 318 F. 3d at 1048–50. Defendant can re-raise this argument on summary judgment upon a developed factual record.

Second, notwithstanding Defendant's status as a consenting party to the communications, Plaintiffs have plausibly alleged that Defendant is not entitled to protection from liability under the crime-tort exception to the ECPA. It is well settled under the ECPA that "it is lawful for an individual to intercept a communication if he is a party to it." *Ramos v. Delphi Behavioral Health Grp., LLC*, 2022 WL 1415856, at *1 (11th Cir. May 4, 2022) (citing 18 U.S.C. § 2511(2)(d))). However, the ECPA's so-called "crime-tort" exception allows a plaintiff to state a claim under the ECPA in spite of a defendant's consent to the communications, if the plaintiff plausibly alleges that the communications were "intercepted for the purpose of committing any criminal or tortious act . . . ." 18 U.S.C. § 2511(2)(d).[8] That pocket of liability for tortious consented-to interceptions plausibly applies here, at least to withstand dismissal under Rule 12(b)(6), given Plaintiffs' allegation that Defendant and the third parties knowingly intercepted Plaintiffs' electronic

[8] The full provision at issue states as follows:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C.A. § 2511(2)(d).

communications without Plaintiffs' consent to "exploit the confidential communications for targeted advertisements and direct marketing," and in violation of state privacy laws [ECF No. 21 ¶ 140]. Defendant may re-raise this argument on summary judgment. *See W.W. v. Orlando Health, Inc.*, No. 6:24-CV-1068, 2025 WL 722892, at *10 (M.D. Fla. Mar. 6, 2025) ("Application of the crime-tort exception [is] more fit for resolution at summary judgment or trial than at the motion to dismiss stage.").

Count I may proceed.

III. Plaintiffs state a claim under Cal. Penal Code Sections 631 and 632 but fail to state a claim under Cal Penal Code Section 502.

A. Plaintiffs state a claim under Cal. Penal Code § 631 (Count II).

Count II is brought under the wiretap provision of the CIPA. Cal. Penal Code §§ 631(a). That statute creates civil liability against a defendant who "by means of any machine, instrument, or contrivance . . . willfully and without consent . . . 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 who aids, agrees with, employs, or conspires with any person . . . to unlawfully do [so]." Cal. Penal Code §§ 631(a), 637.2(a).

Defendant seeks dismissal of Count II, chiefly arguing that Plaintiffs cannot state a claim under that statute because they do not plausibly allege that the third parties acquired the "contents" of Plaintiffs' communications [*see* ECF No. 23 pp. 9–11].[9] Plaintiffs say otherwise, asserting that

[9] Defendant also maintains, similar to its argument regarding interception as to Count I, that Plaintiffs' communications were not intercepted "in transit" within the meaning of CIPA [ECF No. 23 pp. 9–11]. This argument fails at this stage for similar reasons as stated above in reference to the contemporaneous-interception requirement under the ECPA. Cal. Penal Code §§ 631(a); *People v. Malotte*, 292 P.2d 517, 520, 520 n.1 (Cal. 1956) (applying a contemporaneous interception standard to the language now found in CIPA section 631(a)); *see also Pena v GameStop, Inc.*, 670 F. Supp. 3d 1112, 1120 (S.D. Cal. 2023) ("CIPA's 'while the same is in transit' language has the same effect [as the 'intercept' requirement in the ECPA], and courts look to cases

Defendant intercepted the "contents" of their communications by facilitating the capture and disclosure of specific types of substantive information—"form field entries," "the text of buttons clicked," and "full-string URLs" [ECF No. 34 p. 11].

To decipher whether Defendant acquired the "contents" of Plaintiffs' communications, the Court begins with the ordinary meaning of the word "contents" in 1968 at the time of CIPA's enactment. Though CIPA does not define the word "contents," the ECPA does, and courts routinely look to the ECPA in interpreting CIPA language because both statutes are similarly worded, serve similar functions, and were passed within a year of each other. *See, e.g.*, *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) ("The analysis for a violation of [the] CIPA is the same as that under the federal Wiretap Act."). The ECPA defines "contents" as "any information concerning the substance, purport, or meaning of [a] communication." *See* 18 U.S.C. §§ 2510(8), 2711(a). "A dictionary from 1968 defines 'substance' to mean '[e]ssence; the material or essential part of a thing,' 'purport' to refer to '[m]eaning; import; substantial meaning; substance,' and 'meaning' to refer to '[t]hat which is, or is intended to be, signified or denoted by act or language.'" *W.W. v. Orlando Health, Inc.*, No. 6:24-CV-1068, 2025 WL 722892, at *5 (M.D. Fla. Mar. 6, 2025) (quoting *Substance, Purport, Meaning*, Black's Law Dictionary (4th ed. 1968)).[10]

Courts have expounded on CIPA's "content" requirement. Content is distinguishable from "non-content" or "record information" about a communication, such as "extrinsic information used to route a communication," which is not actionable if collected. *In re Google*, 806 F.3d at 135–

analyzing the [ECPA] in applying CIPA's 'in transit' requirement."); *Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072, 1084 (C.D. Cal. 2023) (collecting cases).

[10] "A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning." *Perrin v. United States*, 444 U.S. 37, 42 (1979).

136. That is because "[c]omputer users . . . have no reasonable expectation of privacy in electronic data that is not itself content." *People v. Evensen*, 208 Cal. Rptr. 3d 784, 790 (Cal. Ct. App. 2016). "For instance, information about a telephone call's origination, length and time have been found to be non-content record information." *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1083 (N.D. Cal. 2015) (quotation omitted). But "record information may constitute 'contents' where the record is the subject of a communication." *Price v. Carnival Corp.*, 712 F. Supp. 3d 1347, 1360 (S.D. Cal. 2024) (quotation omitted). That includes, for example, inputting information—including contact information, like "email addresses" and "telephone numbers"—"into a form provided by a website." *In re Zynga Priv. Litig.*, 750 F. 3d 1098, 1107 (9th Cir. 2014); *see also In re Pharmatrak*, 329 F. 3d 9, 16 (1st Cir. 2003) (finding the "contents" of communications includes "personal information entered into an online form").

Applying these principles to the First Amended Complaint, Plaintiffs have sufficiently alleged that the third parties' software intercepted their content-based searches and web-activity. Plaintiffs allege that Defendant assisted the third parties with intercepting the following information: 1) "form field entries"; 2) "the text of buttons clicked"; and 3) "full-string URLs" that reveal "a user's search queries" and "the precise file requested" [*see, e.g.*, ECF No. 21 ¶¶ 7–9, 48, 52, 92, 102, 135, 138]. For instance, Plaintiffs allege the third party software on Defendant's website tracks the name of the precise file requested [*see, e.g.*, ECF No. 21 ¶ 47 ("1800pedmeds.com/*nexgard+chewables*-10372.html" (emphasis added))], tracks what medications are being "added to the cart" [ECF No. 21 ¶ 50–52], and tracks user information entered into "form fields" [ECF No. 21 ¶ 61]—and then takes that information and pairs it with the relevant Facebook user's page or user profile [ECF No. 21 ¶¶ 53–61; *see also* ECF No. 21 ¶¶ 90–107 (similar allegations against Attentive and Zeta)]. On those accepted facts, the Court

finds that Plaintiffs' form entries, text of buttons clicked, and full string URL's reveal the "substance," "purport," and/or "meaning" of their communications—at least for purposes of Rule 12(b)(6). Framed differently, it is plausible that the value of the communications lies in the purchase selections and form entries themselves—i.e., in the substantive information contained therein—not simply in the routing information automatically generated at the point Plaintiffs' communications were shared.[11] Net-net, the third parties are not merely tracking "record-based" information like dates and times visited on Defendant's website, but instead are tracking at least some portion of the "essence" of the communications, including information related to Plaintiffs' pets' medical conditions. *See Substance, Purport, Meaning*, Black's Law Dictionary (4th ed. 1968).

Count II under CIPA § 631 may proceed.

B. Plaintiffs state a claim under Cal. Penal Code § 632 (Count III).

Count III is brought under the eavesdropping provision of the CIPA, which creates civil liability against a defendant who "intentionally and without . . . consent . . . uses an electronic amplifying or recording device to eavesdrop upon or record [a] confidential communication . . . ." Cal. Penal Code §§ 632(a), 637.2(a).

[11] Other courts have reached similar conclusions regarding the "content-based" nature of similar material. *See, e.g.*, *In re Grp. Health Plan Litig.*, 709 F. Supp. 3d at 712, 718, 720 (determining that "a URL that discloses a search term or similar communication made by the user can be considered a [content] communication under the [ECPA]" (quotation omitted)); *Doe v. Microsoft Corp.*, No. C23-0718, 2023 WL 8780879, at *9 (W.D. Wash. Dec. 19, 2023) ("[The p]laintiff alleges [the defendant] collects URLs containing search queries that could divulge a user's medical conditions, allergies, and immunizations. Accordingly, [the p]laintiff has adequately pled that [the defendant] intercepted the contents of her communication with [a healthcare provider] for purposes of [the] CIPA." (citation omitted)).

Defendant challenges Count III on the following basis: Plaintiffs' communications with Defendant's website were not "confidential communication[s]" within the meaning of the CIPA because Plaintiffs did not have a reasonable expectation of privacy in their easily shared online communications [ECF No. 23 p. 13]. Plaintiffs reject this view, characterizing the communications as containing private veterinarian information that were not to be disclosed to any party other than Defendant [ECF No. 21 ¶¶ 154–158].[12]

CIPA's eavesdropping provision defines "confidential communication" as:

> any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive, or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

Cal. Penal Code § 632(c). To be "confidential" under this provision, therefore, any party to that communication must have "an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 41 P.3d 575, 582 (Cal. 2002).

Internet-based communications which can easily be shared by the recipient of the communication, such as communications on instant messenger chats, are not confidential within the meaning of section 632. *See, e.g.*, *People v. Nakai*, 107 Cal. Rptr. 3d 402, 418 (Cal. Ct. App. 2010) (holding that Yahoo chats were not confidential because chats can easily be printed, shared, or forwarded to a third party); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014) (holding the same regarding Facebook chat messages). On the other hand, sensitive medical

[12] Aiders and abettors of a violation of section 632 "commit the violation . . . as much as the perpetrator does." *Nagy v. Whittlesey Auto. Grp.*, 47 Cal. Rptr. 2d 395, 398 (Cal. Ct. App. 1995) (quotation omitted) (holding that section 632 supports derivative liability); *Smith v. Rack Room Shoes, Inc.*, No. 24-CV-06709, 2025 WL 1085169, at *5 (N.D. Cal. Apr. 4, 2025) (same).

communications which are protected by state or federal law can be deemed confidential and subject to protection under section 632. *See, e.g.*, *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 799 (N.D. Cal. 2022) (holding that communications were confidential under section 632 where the communications were "protected by federal law" and were "uniquely personal," "health-related communications").

Here, Plaintiffs have done enough to plausibly allege that their communications to Defendant were made in circumstances they "desire[d] [] to be confined to the parties thereto," at least with respect to the veterinary prescription information at issue. Cal. Penal Code § 632(c). Plaintiffs allege throughout their complaint that, in visiting Defendant's website, they "expected that communications revealing [their private] information would remain confidential" [ECF No. 21 ¶¶ 7–9]. More specifically, Plaintiffs explain that Defendant represented to them, in a hyperlink on the checkout page on its website, that "[a]ll personal and prescription information is securely managed and treated with the highest level of confidentiality, regardless of the processing location" [ECF No. 21 ¶ 30]. Having seen such a disclosure, Plaintiffs reasonably could have expected that their personal and prescription information would be "confined to the parties thereto." Cal. Penal Code § 632(c). And, as an additional contextual point, state law prohibits pharmacies—including those that dispense veterinary medicine like Defendant—from "exhibit[ing], discuss[ing], or reveal[ing] the contents of any prescription, the therapeutic effect thereof, the nature, extent, or degree of illness suffered by any patient or any medical information furnished by the prescriber" [*see* ECF No. 21 ¶¶ 22–23 (quoting Cal. Code Regs. Tit. 16 § 1764 and Cal. Bus. & Prof. Code § 4040(2))]. Against this backdrop, the Court will permit Count III to proceed.[13]

[13] Defendant also argues that the Complaint does not allege that PetMed had the requisite intent to aid and abet a Section 632 CIPA violation [ECF No. 23 p. 13–14]. Plaintiffs allege, however, that Defendant intentionally integrated the computer code that intercepted electronic communications

C. Plaintiffs fail to state a claim under Cal. Penal Code § 502 (Count IV).

Plaintiffs bring Count IV under the Comprehensive Computer Data and Access and Fraud Act ("CDAFA"). That statute creates civil liability against a defendant who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network . . . whether existing or residing internal or external to a computer, computer system, or computer network." Cal. Penal Code §§ 502(c)(2), 502(e)(1). Importantly, the CDAFA creates a cause of action only for owners of data "who suffer[] damage or loss by reason of a violation" of the statute. *See* Cal. Penal Code § 502(e)(1).

Pointing to the language requiring Plaintiff to demonstrate "damage or loss" to recover under the CDAFA, Cal. Penal Code § 502(e)(1), Defendant argues that Plaintiffs have not demonstrated a cognizable loss, such as economic harm to them, resulting from the allegedly disclosed data [ECF No. 21 pp. 16–17; ECF No. 35 p. 9]. In response, Plaintiffs characterize their data as inherently valuable, further stating that Defendant caused the third parties to profit off of Plaintiffs' private information, which Plaintiffs could have independently sold themselves [*see* ECF No. 21 ¶¶ 159–67].

Federal district courts appear to be split regarding whether a plaintiff may sustain a CDAFA claim in cases involving re-routing of personal data where a market exists for such data but the data owner does not suffer an actual personal loss or harm from the unlawful use of such data.[14]

---

from Plaintiffs and Class members while they accessed and navigated Defendant's website [*see, e.g.*, ECF No. 21 ¶ 87]. Just like the crime-tort exception discussed in Part II, *supra*, this contested question of intent is better decided following discovery. *See, e.g.*, *In re Grp. Health Plan Litig.*, 709 F. Supp. 3d at 712, 718, 720 ("This case is at the pleading stage. While [the p]laintiffs have alleged [the defendant's] motivations, determination of [the defendant's] actual purpose for installing and using the Pixel Code requires a factual undertaking.").

[14] The parties do not cite any controlling California law addressing the loss/damage issue under the CDAFA [ECF No. 21 pp. 16–17; ECF No. 34 pp. 18–19; ECF No. 35 p. 9].

Compare Cottle v. Plaid Inc., 536 F. Supp. 3d 461, 488 (N.D. Cal. 2021) ("Plaintiffs offer no support for their theories that the loss of the right to control their own data, the loss of the value of their data, and the loss of the right to protection of the data, as discussed above, is 'damage or loss' within the meaning of the CDAFA."), *with Rodriguez v. Google LLC*, 772 F. Supp. 3d 1093, 1110 (N.D. Cal. 2025) ("[A] reasonable juror could find that plaintiffs suffered damage or loss because [defendant] profited from the misappropriation of their data.").

Without any identified binding California precedent, the Court begins and ends with the text of the statute, which requires the owner of the data to suffer "damage or loss by reason" of the taking and use of computer data. *See* Cal. Penal Code § 502(e)(1). Even accepting Plaintiffs' allegations as true, Plaintiffs have not plausibly alleged such damage or loss. Plaintiffs do not allege that they suffered any actual financial or economic harm resulting from the challenged interception and disclosure of their data. They do not allege that they were ever in the business of selling or profiting off of their data. And they do not allege that anyone ever offered to buy or collect their consumer data. At most, Plaintiffs proffer a disgorgement theory based on equitable principles in California law—alleging that "[c]ompanies view [their private] information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information" [ECF No. 21 ¶ 108 (quotation omitted); ECF No. 21 ¶¶ 109–110 (describing several studies in which third parties like Meta paid consumers for a license to collect their browsing data)].[15] But even accepting that theory as true, both empirically and as a matter of equity, it is not enough to satisfy what matters here—which is the statutory requirement in the CDAFA that *the*

[15] *See also Cty. of San Bernardino v. Walsh*, 69 Cal. Rptr. 3d 848, 856 (Cal. Ct. App. 2007) (noting that where "a benefit has been received by the defendant but the plaintiff has not suffered a corresponding loss, or in some cases, any loss, but nevertheless the enrichment of the defendant would be unjust . . . [t]he defendant may be under a duty to give to the plaintiff the amount by which [the defendant] has been enriched" (quotation omitted))].

data owner herself suffer some non-speculative damage or loss resulting from the use or disclosure of the subject data. *Cottle*, 536 F. Supp. 3d at 488. On that issue, Plaintiff's First Amended Complaint is bare, asserting no concrete damage or loss to the Plaintiffs' themselves resulting from the alleged statutory violation—and ultimately leaving Plaintiff with nothing more than hypothetical harm in the value of their data on the open market. *See Lineberry v. AddShopper, Inc.*, No. 23-CV-01996-VC, 2025 WL 551864, at *2 (N.D. Cal. Feb. 19, 2025) (dismissing similarly speculative economic loss theory on CDAFA statutory standing). This Court will not expand the plain meaning of "damage or loss" for Plaintiffs' disgorgement theory on such speculative grounds. Accordingly, Count IV must be dismissed.

IV. Plaintiffs have not stated a claim for intrusion upon seclusion (Count V).

Plaintiffs' last claim alleges common law intrusion upon seclusion against Defendant. At common law, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B.[16]

[16] The parties do not agree on whether Florida or California substantive law applies to this claim [ECF No. 23 p. 17 (arguing Florida law applies); ECF No. 34 p. 19 (arguing California law applies)]. As a federal court sitting in diversity jurisdiction, the Court applies Florida's "significant relationships test" to resolve tort conflict-of-law issues. *Bishop v. Florida Specialty Paint Co.*, 389 So. 2d 999, 1001 (Fla. 1980). At first blush, it appears California law should apply; Plaintiffs were injured in California, and California is, after all, where Defendant caused Plaintiff's browsers to transmit the confidential information. *C.f. Binion v. O'Neal*, No. 15-60869-CIV, 2016 WL 111344, at *2–*3 (S.D. Fla. Jan. 11, 2016) (applying Michigan law when a Plaintiff who lived in Michigan was injured by a social media tweet posted in Florida); *Popa v. Harriet Carter Gifts, Inc.*, 52 F. 4th 121 (3d Cir. 2022) (holding that a defendant intercepted electronic communications "at the point where it routed those communications to its own servers" from the plaintiff's browser, not where the signals were received at [the defendant's] servers"). Regardless, as stated below, the Court need not make a choice of law determination here because the result is the same under the law of either jurisdiction.

Though the parties do not agree as to whether Florida or California applies to Plaintiffs' intrusion upon seclusion claim, both states require the intrusion upon seclusion to be "highly offensive to a reasonable person." *Jackman v. Cebrink-Swartz*, 334 So. 3d 653, 656 (Fla. Dist. Ct. App. 2021) (determining that plaintiffs could establish a likelihood of highly offensive conduct when the defendant erected a camera to see over a privacy fence and thereafter surveil plaintiffs' residence); *Shulman v. Grp. W Prods., Inc.*, 955 P.2d 469, 490, 494 (Cal. 1998) (holding that plaintiffs plausibly alleged highly offensive conduct when a journalist entered and rode in an ambulance with two seriously injured patients).

As a matter of law, Plaintiffs have not met that "highly offensive" bar in this case. Notwithstanding Plaintiffs' lofty rhetoric [*see* ECF No. 34 pp. 19–20], the conduct at issue here is not highly offensive under any understanding of the common law tort. Indeed, there is no meaningful dispute, nor could there be, that the use of cookies on commercial websites for adults is widespread and commonplace. *See generally In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 294–95 (3rd Cir. 2016). And while the Court has determined in this Order, for purposes of Rule 12(b)(6), that Plaintiffs have alleged a sufficient privacy interest in their pets' veterinarian information and related keystrokes, links, and form entries, that interest simply cannot be equated with the sorts of offensive intrusions that have triggered liability under the common law (like the disclosure of intimate photographs or medical information concerning human patients). *See* Restatement (Second) of Torts § 652B, cmt. b; *see also Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1127 (S.D. Cal. 2023); *cf. Tucker v. John R. Steele & Assocs., Inc.*, No. 93 C 1268, 1994 WL 127246, at *3 (N.D. Ill. Apr. 12, 1994) ("[T]he reasons for seeking veterinary care and the medical condition of an animal are of an entirely different nature from the personal privacy of one's own health."). More generally, the conduct at issue here is not "so outrageous in character,

and so extreme in degree, as to go beyond all possible bounds of decency." *Stoddard v. Wohlfahrt*, 573 So. 2d 1060, 1062 (Fla. Dist. Ct. App. 1991. Nor does it amount to an "egregious breach of social norms." *Hernandez v. Hillsides, Inc.*, 211 P.3d 1063, 1080 (Cal. 2009).

For these reasons, Plaintiffs' intrusion upon seclusion claim is due to be dismissed.

V. **Plaintiffs have plausibly alleged that they did not consent to the alleged interceptions**.

In a last-ditch effort to dismiss Plaintiffs' claims, Defendant argues that Plaintiffs consented to the alleged interceptions [*see* ECF No. 23 pp. 14–16]. If true, that would bar Plaintiffs' ECPA claim (Count I), and both CIPA claims (Counts II and III). *See* 18 U.S.C. § 2511(2)(c) (exempting from liability communications where "one of the parties to the communication has given prior consent to such interception"); Cal. Penal Code § 631(a) (imposing liability only for interceptions "without the consent of all parties."); Cal. Penal Code § 632(a) (imposing liability only when a party has an objectively reasonable expectation the conversation is not being overheard or recorded).[17]

In support of its argument that Plaintiff consented to the interceptions at issue, Defendant points to its publicly posted Privacy Policy, which notifies web users that it uses "tracking tools including cookies, web beacons or other online information-gathering tools that collect information," that it "partner[s] with third party advertising companies," and that it shares personal information "[w]ith third parties who . . . help us to administer our website, collect data for analysis purposes, conduct surveys, provide technical support, process payments, [and] provide marketing

[17] Consent would also bar Plaintiffs' CDAFA claim and Plaintiffs' intrusion upon seclusion claim, both of which the Court has dismissed on other grounds. Cal. Penal Code § 502(c)(2) (imposing liability only where the access is "without permission"); Restatement (Second) of Torts § 892A ("One who effectively consents to conduct of another intended to invade his interests cannot recover in an action of tort for the conduct or for harm resulting from it.").

research and assistance (including email and mobile marketing)" [ECF No. 23 p. 14; ECF No. 23-1]. Defendant also says that its website features a "consent banner" informing users that they can "opt-out of our making available to third parties information relating to cookies and similar technologies for advertising purposes" [ECF No. 23 p. 14]. Plaintiffs retort that they never assented to Defendant's Privacy Policy, and that they were not on actual or constructive notice of those terms [ECF No. 34 p. 14].

The parties agree that, in determining whether a plaintiff was on notice of a data-sharing advisal, courts consider "the visual design of the webpages," including "whether an advisal is displayed in a font size and format such that the court can fairly assume that a reasonably prudent Internet user would have seen it."[18] *Godun v. JustAnswer LLC*, 135 F. 4th 699, 709 (9th Cir. 2025); [ECF No. 23 pp. 14–15; ECF No. 34 p. 18; ECF No. 35 pp. 7–9]. Importantly, courts also consider the frequency and prominence of the advisal throughout the website and the browsing experience. *See, e.g.*, *Lakes v. Ubisoft, Inc.*, 777 F. Supp. 3d 1047 (N.D. Cal. 2025). For example, in *Lakes*—a case similar to this one involving third party data collection—the court dismissed a plaintiff-class's federal and state wiretapping claims based on the plaintiffs' implied consent to third party interception of their data, because: (1) a cookies banner confronted plaintiffs arriving to a defendant's website and notified them that their data would be sent to third parties; (2) plaintiffs had to create an account and accept defendant's Privacy Policy before making any purchases; and (3) plaintiffs were again presented with the Privacy Policy during every store checkout process. *Id.* at 1054–57.

[18] The parties treat the matter of consent, and the applicable law, in combined fashion across all claims, citing a smattering of mostly federal California caselaw. Seeing no material distinction between the applicable consent authorities, the Court follows that approach as well.

Considering the record at this point, the Court sides with Plaintiffs and concludes that they have sufficiently alleged that they did not consent to the interceptions at issue. Plaintiffs explicitly disclaim actual or constructive notice, alleging that "[a]t no point during the transaction does Defendant put consumers on notice of a privacy policy or terms of service" [*see* ECF No. 21 ¶ 65]. In response, Defendant points the Court to *Lakes*—but that case is a far cry from this one, and it illustrates why dismissal on a consent-basis is inappropriate here at the pleading stage. Though Defendant argues that its privacy policy is "publicly posted" [ECF No. 23 p. 2], the record does not indicate whether customers are ever directed to that policy before clicking links on Defendant's site that are transmitted to the third parties; when (or how often) Defendant's alleged "consent banner" pops up; what the font size or the format is pertaining to the advisal; whether Defendant's users need to create an account to make purchases; or whether users are provided with the privacy policy during checkout.

In sum, the question of consent on Defendant's website is not suitable for resolution at this stage in light of Plaintiff's allegations [*see* ECF No. 21 ¶ 65]; *see Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 601 (N.D. Cal. 2021) ("[T]he mere existence of a privacy policy is not dispositive because users might lack actual or constructive notice of the policy.").[19]

CONCLUSION

For the foregoing reasons, it is hereby **ORDERED AND ADJUDGED** as follows:

[19] Defendant's argument that Plaintiffs consented to the transmission of their data by signing up for Facebook is unavailing in the face of Plaintiffs allegations that "Meta expressly warrants the opposite," promising consumers that "partners" like Defendant cannot use Meta's tools without "hav[ing] lawful rights to collect, use and share [consumers'] data" [*see* ECF No. 21 ¶¶ 66–73]. And, even if the Court were persuaded, that argument still does not address the two other third parties in the Complaint.

1. Defendant's Motion to Dismiss [ECF No. 23] is **GRANTED IN PART AND DENIED IN PART** in accordance with this Order.
2. Plaintiffs' CDAFA and intrusion upon seclusion claims (Counts IV and V) are **DISMISSED WITH PREJUDICE**.[20]
3. Counts I, II, and III may proceed, consistent with this Order.
4. Defendant shall Answer Plaintiff's Complaint [ECF No. 21], as limited by this Order, on or before **February 4, 2026**.

ORDERED in Chambers at Fort Pierce, Florida, this 14th day of January 2026.

AILEEN M. CANNON
UNITED STATES DISTRICT JUDGE

[20] Plaintiffs have not filed a motion to amend or even requested leave to amend within their opposition or surreply [ECF Nos. 34, 40]. Nor does the Court see a basis to warrant a second amendment, either under the more liberal standard under Fed. R. Civ. P. 15 or the applicable good-cause standard for modifying a scheduling order [ECF No. 21 (setting August 11, 2025, as deadline to move to amend pleadings)].