UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

BRANDON BRISKIN,

Plaintiff,

v.

SHOPIFY INC., et al.,

Defendants.

Case No. 21-cv-06269-PJH

ORDER RE DEFENDANTS' MOTION TO DISMISS SECOND AMENDED COMPLAINT

Re: Dkt. No. 84

Defendants' motion to dismiss plaintiff's second amended complaint ("SAC") came on for hearing before this court on December 4, 2025. Plaintiff appeared through his counsel, Stephen Raab, Rajiv Thairani, and Seth Safier. Defendants Shopify Inc, Shopify (USA) Inc., and Shopify Payments (USA) Inc. (collectively, "Shopify") appeared through their counsel, Benedict Hur and Tiffany Lin. Having read the papers filed by the parties and carefully considered their arguments and the relevant legal authority, and good cause appearing, the court hereby rules as follows.

BACKGROUND

This putative class action for invasion of privacy concerns the collection of consumer data over an online shopping platform. Plaintiff Brandon Briskin is an Internet shopper and resident of Madera, California. SAC ¶ 8. Defendant Shopify Inc. is a Canadian company headquartered in Ottawa, Canada. SAC ¶ 9. Defendant Shopify (USA) Inc. ("Shopify USA") is a Delaware company with its principal place of business in Ottawa, Canada. SAC ¶ 14. Defendant Shopify Payments (USA) Inc. ("Shopify Payments") is a Delaware company with its principal place of business in Wilmington,

Delaware. SAC ¶ 15. Both Shopify USA and Shopify Payments are wholly owned subsidiaries of Shopify Inc.

A. Allegations of defendants' collection and use of consumer data

Defendants run an e-commerce platform that provides payment processing services to millions of merchants across the Internet. SAC ¶ 24. Defendants host merchants' websites in addition to facilitating and verifying customers' payment information. SAC ¶ 24. Plaintiff alleges that when a consumer begins the checkout process with one of Shopify's merchant customers, the merchant's software makes it appear that the consumer communicates directly with the merchant, but in reality, the consumer does not send any information to the merchant. SAC ¶¶ 1-2, 4, 25-35, 82. Rather, it is Shopify's software that generates the payment form and collects all information entered into it. Id. Plaintiff complains that Shopify also installs cookies on users' browsers to track consumers' transactions across the Shopify merchant network. SAC ¶¶ 5, 38-41.

In June 2019, plaintiff purchased fitness apparel from IABMFG, a Shopify Inc. merchant, through IABMFG's website. SAC ¶ 57. Plaintiff alleges that he, like other consumers, was uninformed of defendants' involvement in the transaction, and without consent, defendants collected his sensitive private information, including full name, address, email address, credit card number, IP address, the items purchased, and geolocation. SAC ¶¶ 2-3, 40, 81. Defendants take additional steps to use consumer data and make it profitable for themselves and their merchants by compiling the data into individualized profiles. SAC ¶¶ 6, 42-45. Defendants share information within the profiles of consumers with their merchants. Id. The information is valuable to the merchants because they provide insights into consumers' creditworthiness before the transaction is final. Id.

When a consumer makes a purchase, defendants use the consumer's data to provide their merchants with an "analysis" of the order that cross-references the details of the new transaction with the consumer's purchase history to identify potential areas of

fraud. SAC ¶ 43. In addition to building profiles and analyzing their data, defendants share consumer data with other non-merchant third-parties, such as Stripe and MaxMind, who, in turn, use the data to feed their own profiles on consumers. SAC ¶¶ 15-16, 46-47.

B. Plaintiff's Claims

Plaintiff alleges that he never granted consent for defendants to collect and use his data in the methods described above. He alleges that, when he bought an item from IABMFG in 2019, he had no reason to know that Shopify was involved in the transaction or that it would intercept his information. He claims that he did not learn about Shopify's involvement until 2021, at which time the involvement was disclosed in IABMFG's own privacy policy.

Plaintiff seeks to represent a class of similarly situated consumers. His proposed class definition is as follows: "All natural persons who, between August 13, 2017 and the present, submitted payment information via Shopify's software while located in California." SAC ¶ 68. The SAC brings the following claims on behalf of plaintiff and the proposed class against all three defendants, all under California law:

1. Violation of the California Invasion of Privacy Act ("CIPA"), California Penal Code § 631;
2. Violation of the California Invasion of Privacy Act, California Penal Code § 635;
3. Invasion of Privacy Under California's Constitution;
4. Intrusion Upon Seclusion;
5. Violation of the California Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and
6. Violation of the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq.

C. Procedural History

The original complaint was filed on August 13, 2021. Dkt. 1. Plaintiff then sought leave to file the now-operative second amended complaint, which was granted. Dkt. 43 and 44.

In response to the second amended complaint, defendants moved to dismiss, and the court granted dismissal based on lack of personal jurisdiction. Plaintiff appealed and a panel of the Ninth Circuit affirmed. Subsequently, the Ninth Circuit issued an en banc opinion reversing the court's decision re lack of personal jurisdiction and remanding the case for further proceedings. Defendants now move to dismiss the complaint on grounds other than personal jurisdiction.

DISCUSSION

A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) tests for the legal sufficiency of the claims alleged in the complaint. Ileto v. Glock Inc., 349 F.3d 1191, 1199-1200 (9th Cir. 2003). Under Federal Rule of Civil Procedure 8, which requires that a complaint include a "short and plain statement of the claim showing that the pleader is entitled to relief," Fed. R. Civ. P. 8(a)(2), a complaint may be dismissed under Rule 12(b)(6) if the plaintiff fails to state a cognizable legal theory, or has not alleged sufficient facts to support a cognizable legal theory. Somers v. Apple, Inc., 729 F.3d 953, 959 (9th Cir. 2013).

Defendants' motion seeks dismissal of all six asserted claims, and some of their arguments cut across multiple claims, while other arguments are claim-specific. The court will start with the arguments that cut across multiple claims.

A. Rule 9(b)

Defendants argue that all of plaintiff's claims sound in fraud and are therefore subject to Rule 9(b)'s heightened pleading standards. See Dkt. 84 at 14-15. Defendants' argument is that plaintiff's complaint "spins a theory of deception and concealment" by defendants, thus triggering the higher pleading standard.

However, even in defendants' primary supporting case, the court ultimately chose not to apply the Rule 9(b) standard in a data privacy case. See Doe I v. Google LLC, 741 F.Supp.3d 828, 843 (N.D. Cal. 2024). This court finds that decision persuasive and will analyze plaintiff's claims under Rule 8.

B. Statute of limitations

Next, defendants argue that the first four of plaintiff's claims are barred by the relevant statutes of limitation, based on this timeline: plaintiff made his online purchase from a Shopify merchant in June 2019, his counsel visited that website in April 2021, and this lawsuit was filed in August 2021. See Dkt. 84 at 15-17. Defendants argue that plaintiff "does not plead the time and manner of discovery," because while he alleges that "he neither knew nor could have known about Shopify's alleged misconduct until 2021," he does not explain how he was able to discover in 2021 facts about Shopify's data collection in 2019.

The court agrees with defendants that there is something unusual about the way that plaintiff describes his discovery of Shopify's alleged 2019 conduct. Plaintiff's account is as follows: he purchased items on the IABMFG website in June 2019, at which time Shopify's data collection was allegedly not disclosed. Then, in April 2021, plaintiff's counsel visited the IABMFG website, which disclosed Shopify's data collection. Based on that 2021 disclosure, plaintiff infers that IABMFG and Shopify must have been engaging in the same conduct in 2019, only without the disclosure that was present in 2021.

Again, while that reasoning has flaws, the court does not necessarily see it as a statute of limitations issue. In the court's view, the issue is not that plaintiff waited too long after learning about Shopify's 2019 conduct, the issue is that plaintiff has still not presented any non-speculative basis for his allegations about that 2019 conduct.

Notably, in the case that this court finds to be the most factually-analogous, the court did not base its dismissal on a statute-of-limitations argument, but instead relied on the more general pleading requirements of Rule 8. See M.D. v. Google, 2025 WL 2710095 (N.D. Cal. Sept. 23, 2025).

The M.D. plaintiffs purchased medication from a website, and their data was shared with Meta and Google. The defendants argued that the plaintiffs consented to the sharing via the seller's privacy policy. The court found that the seller amended its privacy

policy in 2024, and while the pre-amendment policy was not specific enough to establish consent, the post-amendment policy was.

However, the court still dismissed the complaint in its entirety (i.e., for both pre- and post-amendment conduct), explaining as follows:

> More fundamentally, Plaintiffs claims fail because they have not averred that the challenged data sharing practices were in place before Defendants' obtained Plaintiffs' consent to employ them. Plaintiffs became aware that Defendants intercepted their personal information in September 2024, following the August 2024 Privacy Policy's grant of consent for Defendants' conduct. Though they seek to challenge the interception of data reaching back several years, the Complaint lacks any allegations that the data sharing practices to which users consented in August 2024 were previously undertaken. As presently alleged, Plaintiffs' claims fail for want of factual support. Accordingly, Plaintiffs "have not nudged their claims across the line from conceivable to plausible," and their claims, which all rely on the absence of consent, all must face dismissal.

2025 WL 2710095 at *5.

In this court's view, the above rationale applies with equal force to the present case. As in M.D., plaintiff became aware of a website's data sharing practices through the website's own disclosure in 2021, and then alleged that the practices started years before the disclosure. And as in M.D., plaintiff has not yet "nudged [his] claims across the line from conceivable to plausible," and thus, the claims fail "for want of factual support."

Again, this "for want of factual support" basis is not the same as a statute-of-limitations violation. The issue is not that plaintiff obtained factual support about Shopify's 2019 conduct and then waited too long to file a complaint, the issue is that plaintiff has still not provided adequate factual support that the conduct disclosed in 2021 actually took place in 2019 as well.

Accordingly, all of plaintiffs' claims must be dismissed for want of factual support, but the court will provide plaintiff an opportunity to amend the complaint in order to present more factual support for the claims that survive a merits review which follows.

C. Intent

Defendants then argue that the first five of plaintiff's claims (i.e., all but the UCL

claim) should be dismissed "because there is no allegation that Shopify's conduct was willful or intentional." See Dkt. 84 at 17-19. To analyze defendants' argument, the court will start with the elements of each of the five claims.

1. Claim 1: violation of CIPA § 631(a)

CIPA § 631(a) imposes liability on: Any person who, by means of any machine, instrument, or contrivance, or in any other manner, [1] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, [2] or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; [3] or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, [4] or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section . . .

Plaintiff has now clarified that he seeks relief under clauses 2 and 3 of § 631(a). See Dkt. 88 at 20-21.

As noted above, Shopify's argument is that a violation of § 631(a) requires the communications to be accessed "willfully and without the consent of all parties" or otherwise "unauthorized," and that plaintiff cannot establish that element because Shopify's policies required merchants to obtain consent for Shopify's access.

Plaintiff alleges that some of those merchants (such as IABMFG) did not obtain proper consent. However, even taking those allegations as true, Shopify's state of mind is the same, regardless of what merchants like IABMFG ultimately do with their privacy policy. In other words, if we compare two hypothetical scenarios – one where IABMFG obtains proper consent, and one where it doesn't – technically, Shopify's 'intent' is the

same in both scenarios.

Thus, as currently alleged in the complaint, plaintiff's § 631(a) claim fails to adequately allege that defendants acted with the requisite intent to violate the statute. Accordingly, defendants' motion to dismiss claim 1 is granted on that basis. Because the claim could be cured by amendment, it is dismissed with leave to amend.

2. Claim 2: violation of CIPA § 635

CIPA § 635 imposes liability on: "Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones . . ."

Defendants argue that, as with § 631, plaintiff has not adequately alleged intent. However, plaintiff cites a case, which the court finds persuasive, holding that section 635 "does not require intent or knowledge that the device would actually be used unlawfully," and defendants' reply does not adequately rebut that argument. See Dkt. 88 at 27 (citing Yoon v. Meta Platforms, Inc., 2024 WL 5264041 (N.D. Cal. Dec. 30, 2024)).

In the absence of any cited authority holding that section 635 requires intent or knowledge that the device would actually be used unlawfully, the court cannot endorse defendants' argument regarding section 635, and thus denies defendants' motion to dismiss claim 2 on that basis.

3. Claim 3: invasion of privacy, and claim 4: intrusion upon seclusion

The court groups these two claims together because they have similar elements and courts often "consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." See In re Facebook Inc. Internet Tracking Litig., 956 F.3d 589, 605 (9th Cir. 2020).

For background, the elements of invasion of privacy are: (1) a legally protected privacy interest, (2) a reasonable expectation of privacy, and (3) a highly offensive

intrusion. See Hernandez v. Hillsides Inc., 47 Cal.4th 272, 287 (2009).

The elements of intrusion upon seclusion are: (1) a defendant "intentionally intruded into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy," and (2) that the intrusion was "highly offensive" to a reasonable person. See Hernandez at 286.

Although Shopify offers only a single citation for their argument that any violation of these claims must be intentional, the court agrees. See Dkt. 84 at 17 (citing Hayter v. PHH Mortgage Co., 2016 WL 3902483 (N.D. Cal. July 19, 2016) ("The intrusion [upon seclusion] must be intentional.").

Accordingly, as with claim 1, because Shopify's policies required merchants to obtain consent for Shopify's access, plaintiff's claims for invasion of privacy and intrusion upon seclusion fail to adequately allege that defendants acted with the requisite intent to violate the law. Thus, defendants' motion to dismiss claims 3 and 4 is granted on that basis, and claims 3 and 4 are dismissed with leave to amend.

4. Claim 5: CDAFA

CDAFA imposes liability on those who commit the following acts:

> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

Cal. Penal Code § 502(c)(1), (c)(2).

Shopify argues that the terms 'knowingly' and 'without permission' require an intent to access without consent. The words of the statute support that view, as does the cited case law. See People v. Hawkins, 98 Cal.App.4th 1428, 1438-39 (2002) ("The word 'knowing' as used in a criminal statute imports only an awareness of the facts which bring

the proscribed act within the terms of the statute.").

Accordingly, as with claim 1, because Shopify's policies required merchants to obtain consent for Shopify's access, plaintiff's CDAFA claim fails to adequately allege that defendants acted with the requisite intent to violate the law. Thus, defendants' motion to dismiss claim 5 is granted on that basis, and claim 5 is dismissed with leave to amend.

D. Claim-specific arguments

Having addressed defendants' arguments that cut across multiple claims, the court will now address the claim-specific arguments, starting with claim 1.

1. Claim 1: violation of CIPA § 631(a)

As set forth above, CIPA § 631(a) imposes liability on: Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . [2] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; [3] or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained."

Shopify makes two claim-specific arguments: (1) Shopify is an authorized party to the communication, and (2) the complaint does not properly allege that the "contents" of the communications were read "while in transit."

a. Authorized party

Shopify argues that it was simply a 'service provider' for IABMFG, relying on a handful of district court cases, primarily Graham v. Noom, 533 F.Supp.3d 823, 833 (N.D. Cal. 2021). However, plaintiff argues that even Graham recognized that the test for determining whether a defendant is a 'service provider' is whether the defendant uses the data for its own benefit. See Graham at 832 ("Unlike NaviStone's and Facebook's aggregation of data for resale, there are no allegations here that FullStory intercepted

and used the data itself. Instead, as a service provider, FullStory is an extension of Noom." (emphasis added)).

Plaintiff further cites cases holding that a defendant need only be capable of using the data for its own benefit. Shopify's reply argues that "those courts err," positing that the CIPA should be read in a way that "harmonizes" it with the CCPA, and how the court should apply the rule of lenity. In the court's view, whether or not Shopify is a service provider seems to necessitate at least some evidentiary record, and thus, the court declines to grant defendants' motion to dismiss on the basis that Shopify was simply a service provider.

b. "Communications" read while "in transit"

There are two sub-arguments here. First, Shopify argues that the type of content that was intercepted (i.e., name, billing/shipping address, phone number, email, credit card info, purchase info) is not the "content" of a communication – it is simply 'record' information. Second, Shopify argues that the communications were not actually read while "in transit," they were read afterwards, making section 631 inapplicable.

The first argument strikes the court as too far-sweeping. While the court recognizes that information such as 'name' and 'email address' are usually record information (for instance, in an email, clearly the body of the email is the 'contents,' and the name/email address are not), that rationale does not extend to credit card information – especially when the 'communication' is making a purchase. In fact, the 'contents' of an online purchase are essentially (1) the product information, and (2) the payment information – if those aren't the 'contents,' then it's unclear what is. And indeed, plaintiff cites cases saying as much, for instance, holding that '[g]enerally, customer information such as a person's name, address, and subscriber number or identity is record information, but it may be contents when it is part of the substance of the message conveyed to the recipient." See Hammerling v. Google, 615 F.Supp.3d 1069, 1093 (N.D. Cal. 2022). Hammerling further held that 'courts employ a contextual case-specific analysis hinging on 'how much information would be revealed' by the information's

tracking and disclosure." Id. at 1092. The court believes that Shopify's argument re 'contents' reaches too far, and declines to endorse it.

The next argument – read while 'in transit' – is based on the complaint's allegation that the relevant data is encrypted and sent to Shopify's servers, and only read/analyzed after it has been received by Shopify. Plaintiff argues that the "in transit" element is satisfied when it is alleged that the defendant received messages "before or simultaneously with" the intended recipient, and that the complaint allows the inference that the transmission occurs in real time, "but to the extent the court believes that allegations must explicitly state as much, plaintiff can easily amend to add such allegations." See Dkt. 88 at 25, n. 9.

The court agrees with defendants that the complaint does not adequately allege that the contents of the communications were read "in transit," and grants defendants' motion to dismiss claim 1 on that basis, with leave to amend.

2. Claim 2: violation of CIPA § 635

As set forth above, CIPA § 635 imposes liability on: "Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones..."

Defendants argue that section 635 requires plaintiff to show injury from the "manufacture, sale, or assembly of an eavesdropping device," and that it is not enough to show injury from mere "use." See Dkt. 84 at 27 (citing Saleh v. Nike, Inc., 562 F.Supp.3d 503, 522 (C.D. Cal. 2021) ("Contrary to Plaintiff's argument, § 635 does not prohibit the 'implementation' or 'use' of a wiretapping device; instead, it prohibits the manufacture, assembly, sale, offer for sale, advertisement for sale, possession, transport, import, or furnishment of such device.")). Based on that reasoning, the court concludes that the section 635 claim must be dismissed, and because plaintiff cannot amend the complaint

to allege injury through manufacture, sale, or assembly of Shopify's software, the dismissal of section 635 is without leave to amend.

3. Claim 3: invasion of privacy, and claim 4: intrusion upon seclusion

As stated above, the elements of invasion of privacy are: (1) a legally protected privacy interest, (2) a reasonable expectation of privacy, and (3) a highly offensive. intrusion See Hernandez, 47 Cal.4th at 287.

The elements of intrusion upon seclusion are: (1) a defendant "intentionally intruded into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy," and (2) that the intrusion was "highly offensive" to a reasonable person. See Hernandez at 286.

Because the two tests are similar, courts often "consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." See In re Facebook, 956 F.3d at 605.

Shopify's arguments here are all directed to the "highly offensive" prong. See Dkt. 84 at 19. Essentially, Shopify argues that their data collection is the type of routine commercial behavior that would be obvious to anyone who makes online purchases.

However, as explained in the Ninth Circuit's en banc opinion, Shopify's conduct went beyond the type of routine commercial behavior that would be reasonably expected, including that "Shopify surreptitiously implanted cookies that permanently remained on Briskin's device [and] tracked its physical location." See 135 F.4th 739, 745 (9th Cir. 2025).

Moreover, as plaintiff points out, courts are reluctant to conclude, at the pleading stage, that conduct was "highly offensive."

For the foregoing reasons, defendants' motion to dismiss claims 3 and 4 is denied on the bases discussed here.

4. Claim 5: CDAFA

Shopify makes only one claim-specific argument here – no actual damages. The only alleged damages are (1) Shopify's receipt and use of the data without consent, and

(2) an alleged price premium, and Shopify argues that neither are sufficient under CDAFA.

Plaintiff relies primarily on a disgorgement theory, citing Smith v. Rack Room Shoes:

> The SAC plausibly pleads that Plaintiffs suffered compensable "damage or loss" under the meaning of CDAFA. "California law requires disgorgement of unjustly earned profits regardless of whether a defendant's actions caused a plaintiff to directly expend his or her own financial resources or whether a defendant's actions directly caused the plaintiff's property to become less valuable." In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 600 (9th Cir. 2020).
>
> A disgorgement theory can "constitute[ ] an injury sufficient to establish [Article III] standing to bring [a plaintiff's] claims for CDAFA violations." Id. at 601. Plaintiffs have a "stake in the profits garnered" unjustly from their data, and "[u]nder California law, this stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable." That logic applies equally to the issue of whether plaintiffs have suffered "damage" under CDAFA. Plaintiffs are damaged by not having received a share of the allegedly unjust profits generated from their data. That reading is also consistent with CDAFA's statutory purpose. The legislature found that the "protection of ... lawfully created ... computer data is vital to the protection of the privacy of individuals, and made available equitable relief. In light of that intent, Rack Room's alleged unjust profit from the use of Plaintiffs' private personal information, which holds at least some financial value to Rack Room, plausibly constitutes a "damage or loss" within the meaning of CDAFA.

2025 WL 2210002 (N.D. Cal. Aug, 4, 2025).

Smith relies on Ninth Circuit authority in the Facebook Tracking case, which held as follows:

> Because California law recognizes a legal interest in unjustly earned profits, Plaintiffs have adequately pleaded an entitlement to Facebook's profits from users' personal data sufficient to confer Article III standing. Plaintiffs allege that their browsing histories carry financial value. They point to the existence of a study that values users' browsing histories at $52 per year, as well as research panels that pay participants for access to their browsing histories.
>
> Plaintiffs also sufficiently allege that Facebook profited from this valuable data. According to the complaint, Facebook sold user data to advertisers in order to generate revenue. Indeed, as alleged, Facebook's ad sales constituted over 90% of the social media platform's revenue during the

> relevant period of logged-out user tracking.
> …
> Thus, Plaintiffs sufficiently alleged a state law interest whose violation constitutes an injury sufficient to establish standing to bring their claims for CDAFA violations.

956 F.3d 589, 600-01.

That said, Shopify's opening motion does cite other cases that support its view 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" is not a cognizable loss under CDAFA. See, e.g., Cottle v. Plaid, Inc., 536 F.Supp.3d 461, 488 (N.D. Cal. 2021); see also Doe v. County of Santa Clara, 2024 WL 3346257 (N.D. Cal. July 8, 2024); Doe v. Meta Platforms, 690 F.Supp.3d 1064, 1081-82 (N.D. Cal. 2023).

Overall, while the court is unclear about how to square those two lines of cases, it does appear that the Ninth Circuit has concluded that plaintiffs can establish standing for both Article III and CDAFA purposes under a disgorgement theory, and Shopify hasn't presented any convincing reason to contravene that authority. Accordingly, defendants' motion to dismiss claim 5 is denied on that basis.

5. Claim 6: UCL

Shopify argues that plaintiff has no standing under the UCL, and that plaintiff cannot establish any of the unlawful/fraudulent/unfair prongs.

The standing argument is essentially the same as the CDAFA 'no damage/loss' argument. Even though neither of the parties cited it, a recent decision noted that "courts in this district appear split regarding whether privacy harms involving personal data can constitute an injury to money or property sufficient to provide standing under the UCL." Libman v. Apple, 2024 WL 4314791 (N.D. Cal. Sep. 26, 2024). Essentially, some courts have adopted the view that "privacy harms can constitute economic injury to confer UCL standing under three theories: unfair benefit-of-the-bargain to businesses who violate user expectations about how their data will be used, diminished value of personal information, and reduced right to exclude others from accessing personal data," while others have not. See In re Meta Pixel Tax Filing Cases, 2024 WL 1251350, at *24 (N.D.

Cal. Mar. 25, 2024) cf. In re Facebook Priv. Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) ("[P]ersonal information does not constitute property for purposes of a UCL claim").

While the court cannot predict the way in which this split will ultimately be resolved, it is the court's view that smartphones contain so much personal information about their users that the unlawful access of that information can cause harm, even if in a non-monetary way. To require monetary loss would be akin to having a "peeping tom" statute with a "pecuniary loss" requirement.

The court does not endorse the view that the access of any personal information is a per se UCL violation, nor does it endorse the view that personal information access can never be a UCL violation. Accordingly, to the extent that defendants seek dismissal of claim 6 based on the lack of any injury, the motion to dismiss is denied.

CONCLUSION

For the reasons stated above, the court GRANTS in part and DENIES in part defendants' motion to dismiss. Specifically, claim 2 is dismissed without leave to amend. All other claims are dismissed with leave to amend for want of factual support. Claims 1, 3, 4, and 5 are also dismissed with leave to amend to allege facts establishing defendants' intent to access the consumer information without permission.

On all remaining bases, defendants' motion is denied.

Plaintiff shall have 28 days from the date of this order to file a third amended complaint, in accordance with this order along with a redlined version clearly reflecting the changes made. Defendants shall have 21 days thereafter to respond to the third amended complaint.

IT IS SO ORDERED.

Dated: January 21, 2026

/s/ Phyllis J. Hamilton
PHYLLIS J. HAMILTON
United States District Judge