

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

EVELIA RODRIGUEZ, ERIKKA WILSON,
A.N., a minor, AIDEN GUNDLACH, J.V., a
minor, ZACHARY BUCKUS, and RAYMON
MARINES, *individually and on behalf of
all others similarly situated*,

Plaintiffs,

v.

BYTEDANCE, INC., BEIJING DOUYIN
INFORMATION SERVICE CO. LTD.,
BYTEDANCE LTD., BYTEDANCE PTE. LTD.,
BEIJING BYTEDANCE TECHNOLOGY CO.
LTD., and TIKTOK, INC.,

Defendants.

Case No. 23 CV 4953

Hon. Georgia N. Alexakis

MEMORANDUM OPINION AND ORDER

Plaintiffs Evelia Rodriguez, Erikka Wilson, A.N., Aiden Gundlach, Zachary Buckus, Raymon Marines, and J.V. bring this suit individually and on behalf of a putative class against defendant ByteDance, Ltd. (“ByteDance”) and related companies. They allege that defendants violated privacy statutes by collecting their data from a video-editing application called CapCut. Defendants have moved to dismiss the suit on all counts pursuant to Federal Rule of Civil Procedure 12(b)(6). [30]. The Court grants in part and denies in part defendants’ motion to dismiss.

LEGAL STANDARD

A complaint must contain 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 need only

contain factual allegations that, accepted as true, are sufficient to “state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is plausible “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* (citing *Twombly*, 550 U.S. at 556). The allegations “must be enough to raise a right to relief above the speculative level.” *Twombly*, 550 U.S. at 555.

At the pleading stage, a court must “accept all well-pleaded factual allegations as true and view them in the light most favorable to the plaintiff.” *Lavalais v. Vill. of Melrose Park*, 734 F.3d 629, 632 (7th Cir. 2013). But “allegations in the form of legal conclusions are insufficient.” *McReynolds v. Merrill Lynch & Co.*, 694 F.3d 873, 885 (7th Cir. 2012). “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” *Iqbal*, 556 U.S. at 678.

BACKGROUND

For purposes of defendants’ motion to dismiss, the Court accepts as true plaintiffs’ allegations in their amended class action complaint. [22]. *See Felland v. Clifton*, 682 F.3d 665, 672 (7th Cir. 2012).

A. The CapCut App

CapCut is a video-editing application that allows users to create, edit, and customize videos which are often posted on social media platforms such as Instagram and TikTok. [22] ¶ 1. Within the app, users can edit videos with various templates, filters, visual effects, and music. *Id.* Although the app is generally free, users may

obtain access to additional features by paying a monthly or yearly subscription. *Id.* ¶ 66. CapCut has become very popular since it was first introduced to the United States in 2020. It is the fourth most downloaded app in the world and has more than 200 million monthly active users. *Id.* ¶ 2.

CapCut was developed and is run by ByteDance, a Chinese technology company. *Id.* ¶¶ 43, 48. ByteDance also owns TikTok, one of the world’s fastest-growing social media platforms. *Id.* ¶¶ 46–47. In the period leading up to this suit, TikTok reported 150 million monthly active users in the United States. *Id.* ¶ 47. ByteDance directly owns CapCut, but TikTok Inc. is a California corporation and a wholly owned subsidiary of TikTok, LLC, which, in turn, is a wholly owned subsidiary of ByteDance. *Id.* ¶ 29.¹

B. Alleged Privacy Violations

According to plaintiffs, “the CapCut app collects a broad array of private and personally identifiable data and content from which Defendants unjustly profit.” [22] ¶ 100. This includes registration information, phone and social network contacts, identifier and location information, photos and videos, audio data, product integration and usage data, crash data, dump data, performance data, and

¹ With respect to the remaining named defendants: Beijing Douyin Information Service Co. Ltd. (previously named Beijing ByteDance Technology Co. Ltd.) and ByteDance, Inc. are wholly owned subsidiaries of ByteDance. [22] ¶¶ 23, 24, 26. ByteDance Pte. Ltd. is a Singapore private limited liability company. *Id.* ¶ 28. Plaintiffs allege that none of the corporate defendants “function as separate and independent ... entities”; that ByteDance tightly controls TikTok and its other affiliates; and that these entities all “constitute a single enterprise with a unity of interest.” *Id.* ¶¶ 30, 35.

diagnostics data. *Id.* ¶ 103. Plaintiffs also allege that defendants collect face geometry scans and voiceprints from users. *Id.* ¶ 303.

In plaintiffs’ view, defendants “have a history of violating the privacy rights of users of their apps” through questionable data-collection and data-sharing practices. *Id.* ¶¶ 74–75. Although many of the sources plaintiffs cite relate to TikTok’s data practices, plaintiffs contend that “the CapCut app is no less of a threat to the privacy of its users.” *Id.* ¶ 93. Most prominently, plaintiffs allege that ByteDance user data is made available to the Chinese Communist Party (“CCP”) and the Chinese government, thus posing “significant national security concerns.” *Id.* ¶¶ 78–79; *see also* ¶¶ 83–84. According to plaintiffs, “Chinese companies have a legal obligation to cooperate with the Chinese government and provide the government with user data they collect.” *Id.* ¶ 86.

C. Procedural History

In July 2023, Evelia Rodriguez, Erikka Wilson, and A.N. filed a class action complaint against Beijing Douyin Information Service Co. Ltd. f/k/a Beijing ByteDance Technology Co. Ltd.; Beijing ByteDance Technology Co. Ltd.; ByteDance, Inc.; ByteDance Ltd.; ByteDance Pte. Ltd.; and TikTok, Inc. f/k/a Musical.ly, Inc. [1]. In February 2024, these plaintiffs filed an amended class action complaint, this time adding plaintiffs Aiden Gundlach, J.V., Zachary Buckus, and Raymon Marines. [22].

The amended complaint alleges 14 separate privacy-related causes of action under federal, California, and Illinois law. Plaintiffs bring these claims individually

and on behalf of all others similarly situated. *Id.* at 1. In March 2024, defendants moved to dismiss plaintiffs’ amended class action complaint on all counts. [30].

ANALYSIS

The Court first considers defendants’ threshold argument that plaintiffs consented to the collection of their data via CapCut’s Privacy Policy. It then considers whether plaintiffs have stated a claim as to each count in the amended complaint.

A. Consent

Defendants contend that a number of plaintiffs’ claims fail because CapCut’s Privacy Policy discloses plaintiffs’ alleged privacy invasions. [31] at 4–6 & n.3. In support, defendants attach to their motion to dismiss three versions of CapCut’s Privacy Policy, from 2020, 2022, and 2023. *See* [31-1] ¶¶ 4–6; [31-4] Ex. 3; [31-5] Ex. 4; [31-6] Ex. 5. These policies make various disclosures related to the collection of user data. For example, each policy discloses that CapCut collects user-generated content, user registration information, and unique device identifiers. [31-4] Ex. 3 at 14–15, 27–28; [31-5] Ex. 4 at 3–4; [31-6] Ex. 5 at 3–4. The latter two policies also disclose that CapCut “may collect information about the images and audio that are a part of your User Content,” including “identifying the objects and scenery that appear” and “the existence and location within an image of face and body features and attributes.” [31-5] Ex. 4 at 3; [31-6] Ex. 5 at 3.

When a party attaches additional evidence to a motion to dismiss, the general rule is that “the court must either convert the 12(b)(6) motion into a motion for summary judgment under Rule 56 ... or exclude the documents attached to the

motion to dismiss and continue under Rule 12.” *188 LLC v. Trinity Indus., Inc.*, 300 F.3d 730, 735 (7th Cir. 2002) (quoting *Levenstein v. Salafsky*, 164 F.3d 345, 347 (7th Cir. 1998)). However, a “narrow exception” to this rule allows “documents attached to a motion to dismiss [to be] considered part of the pleadings if they are referred to in the plaintiff’s complaint and are central to his claim.” *Id.* (quoting *Wright v. Assoc. Ins. Cos. Inc.*, 29 F.3d 1244, 1248 (7th Cir. 1994)). Here, the requirements for incorporation by reference have been met. Plaintiffs indisputably reference CapCut’s Privacy Policies in their amended complaint, *see* [22] ¶¶ 124, 128–38, and whether these policies constituted plaintiffs’ consent to the alleged data collection is central to their claims that defendants violated various privacy-related statutes.

Even so, whether plaintiffs waived their rights to bring suit based on their alleged consent to CapCut’s Privacy Policy is an affirmative defense that cannot be resolved via this Rule 12(b)(6) motion. *See* Fed. R. Civ. P. 8(c)(1) (listing waiver as an affirmative defense); *Brownmark Films, LLC v. Comedy Partners*, 682 F.3d 687, 690 (7th Cir. 2012) (“[C]ourts should usually refrain from granting Rule 12(b)(6) motions on affirmative defenses.”). Dismissing a claim based on an affirmative defense is only appropriate if “the allegations of the complaint itself set forth everything necessary to satisfy the affirmative defense.” *United States v. Lewis*, 411 F.3d 838, 842 (7th Cir. 2005). Here, several outstanding questions prevent a determination, as a matter of law, that the attached CapCut Privacy Policies “conclusively establish consent.” *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 823 (N.D. Cal. 2020).

None of the materials conclusively establish at this stage of the proceedings when and how plaintiffs agreed to these terms in the CapCut Privacy Policies. Defendants assert that “[u]sers expressly or impliedly consent to the policy upon downloading and using the app,” [31] at 4, but plaintiffs allege that “[d]efendants do not provide such users actual notice of privacy policies or terms of use” and that “[u]sers were able to access the CapCut platform without having to scroll through and read such policies before they were allowed to sign up for the services.” [22] ¶ 130. Although defendants attach to their motion an undated screenshot purporting to show that all users must click “Agree and continue” to CapCut’s Terms of Service and Privacy Policy, *see* [31-9] Ex. 8 at 1, this evidence is insufficient to establish that the named plaintiffs *here* in fact agreed to any terms during the period relevant to this suit. This is especially true where the complaint alleges (and the Court must accept as true) that each named plaintiff never read any privacy policy or terms of use. [22] ¶¶ 10, 13, 16–19.

In addition, plaintiffs assert—and defendants do not dispute—that the attached policies are “only three of the ten (or more) versions of the policy that existed over time.” [36] at 9. The Court thus has no way of knowing whether the named plaintiffs agreed to the attached policies or another version that might contain material differences—a distinct possibility given the differences in the policies defendants have attached. Although the two later policies state that defendants collect a user’s location data, the earlier policy does not. *Compare see* [31-5] Ex. 4 at 4 and [31-6] Ex. 5 at 4, *with* [31-4] Ex. 3 at 14–16; *see also Patterson v. Respondus*,

Inc., 593 F. Supp. 3d 783, 805 (N.D. Ill. 2022) (declining to conclude as a matter of law that written policies on defendant’s webpage governed plaintiffs’ claims because the case “may involve factual questions about what [defendant’s] policies looked like at different moments in time”).

Given these factual issues (and others that may exist), at this stage, CapCut’s Privacy Policies do not preclude plaintiffs’ claims as a matter of law. *See Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 478 (N.D. Cal. 2021) (“The sufficiency of Plaid’s privacy policy is a key disputed issue in this case. Resolution of that issue is inappropriate at this stage.”); *In re Meta Pixel Tax Filing Cases*, 724 F. Supp. 3d 987, 1003 (N.D. Cal. 2024) (“[W]hether plaintiffs consented to having their data collected is a question of fact ... [that] the Court cannot determine at the 12(b)(6) stage.”).

B. Consumer Fraud and Abuse Act (Count I)

The Consumer Fraud and Abuse Act (“CFAA”) imposes liability on a person or entity who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer.” 18 U.S.C. § 1030(a)(2)(C). “[A]n individual ‘exceeds authorized access’ when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him.” *Van Buren v. United States*, 593 U.S. 374, 396 (2021). Section 1030(g) provides that “[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” 18 U.S.C. § 1030(g).

For the reasons explained next, the Court dismisses plaintiffs’ CFAA claim because it does not adequately allege (1) any unauthorized access to particular areas of their devices and (2) “loss” under the CFAA.²

1. Unauthorized Access

Plaintiffs have not met *Twombly*’s pleading standard because, as defendants assert, other than a “barebones assertion that Defendants have the ability to access unnamed files on their devices,” plaintiffs “make no allegation that Defendants accessed any particular areas of their devices outside of the app itself.” [31] at 7.

Plaintiffs’ factual allegations supporting a claim of unauthorized access are limited to the following: “Defendants have built into the CapCut app the capacity to ... access files on user devices and store them,” and “Defendants intentionally accessed Plaintiffs’ devices without the necessary authorization in order to obtain data that Plaintiffs did not authorize them to take.” [22] ¶¶ 105, 157. As for the first allegation, the fact that CapCut had the “capacity” to access files on user devices says nothing about whether defendants did exceed their authorization to access those files. And the second allegation merely recites a required element under § 1030(a)(2). *See Twombly*, 550 U.S. at 555 (“[A] formulaic recitation of the elements of a cause of

² The Court has no reason to address plaintiffs’ argument that they may bring suit when the alleged CFAA violation constitutes “a threat to public health or safety,” 18 U.S.C. § 1030(c)(4)(A)(i)(IV), on the theory that China’s alleged collection of American data via TikTok is such a threat. The Court notes, however, that at least one district court has pointed to an absence of authority to support the suggestion that “because China’s collection of all Americans’ data in the aggregate may pose a threat to national security, every American can assert that the collection of his or her data (no matter the nature of the data) threatens public health or safety under the CFAA.” *See Griffith v. TikTok, Inc.*, No. 5:23-CV-00964-SB-E, 2023 WL 9019035, at *5 (C.D. Cal. Dec. 13, 2023).

action will not do.”) (cleaned up). The complaint otherwise sheds no light on the circumstances surrounding the alleged unauthorized access. It does not specify which area(s) of plaintiffs’ devices defendants supposedly accessed or what type of data defendants sought in exceeding their authorization. Without more, plaintiffs’ factual allegations are not “enough to raise a right to relief above the speculative level.” *Id.* at 555.³

Plaintiffs’ counterarguments are unavailing. They insist that defendants “attempt to rewrite the statute” by focusing on their unauthorized access to “areas” and “files,” rather than “data.” [36] at 11. The battle over terminology is beside the point. To violate § 1030(a)(2)(C), a defendant must “access[] a computer without authorization or exceed[] authorized access.” 18 U.S.C. § 1030(a)(2)(C). Although plaintiffs allege various ways defendants collect and misuse their data, *see, e.g.*, [22] ¶¶ 100–10, the complaint still does not sufficiently allege that defendants “exceeded authorized access” in the process of doing so. 18 U.S.C. § 1030(a)(2)(C).

Leitner v. Morsovillo, 2021 WL 2669547, at *4 (W.D. Mo. June 29, 2021), and *Speed of Light Ops, LLC v. Elliot*, 2023 WL 2815875 (D. Utah Mar. 21, 2023), do not assist plaintiffs either. The allegations in both cases described the specific data defendants accessed without authorization. In *Leitner*, plaintiffs alleged that defendants directed independent contractors “to access and tamper with Plaintiff’s client records and data, with the intent to use that client information to lure away

³ Plaintiffs’ response brief also cites Paragraphs 103, 104, 130, and 158 of the complaint, but besides a few conclusory references to unauthorized access in paragraph 158 (made in the context of loss), these allegations do not support claims of unauthorized access. *See* [22] ¶¶ 103–04, 130, 158.

[plaintiffs] customers.” 2021 WL 2669547, at *2. And in *Speed of Light*, plaintiffs alleged that defendants “had access to certain items under a valid license, and then exceeded that license by manipulating numbers to access other proposals and customer information.” 2023 WL 2815875, at *4. Here, plaintiffs provide the Court with no detail about how defendants exceeded their authorized access to their devices (*i.e.*, what data they accessed).

To be clear, the Court does not base its conclusion on a finding that CapCut was *in fact* authorized to access certain areas of plaintiffs’ devices, as defendants suggest in their opening brief. [31] at 7–8. Factual disputes such as the scope of defendants’ access are not appropriately resolved on a motion to dismiss. *See Leitner*, 2021 WL 2669547, at *4. And defendants’ citation to *Brodsky* does not suggest otherwise. *See Brodsky v. Apple Inc.*, No. 19-CV-00712-LHK, 2019 WL 4141936 (N.D. Cal. Aug. 30, 2019). In that case, plaintiffs’ complaint “concede[d] that [they] voluntarily installed the software update,” which unambiguously established authorization to install two-factor authentication on their devices. *Id.* at *8. Here, questions of fact exist as to the scope of the authorization and the design of plaintiffs’ operating systems. *See, e.g.*, [31] at 7–8 (maintaining that the operating systems “are designed to block any unauthorized access outside of the app”).

Still, this factual dispute over the scope of defendants’ authorized access does not absolve plaintiffs of their burden to plead facts that “nudge their claims across the line from conceivable to plausible.” *Twombly*, 550 U.S. at 570. Because they have

not adequately pled unauthorized access, plaintiffs fail to state a claim under the CFAA.

2. Loss

Plaintiffs' CFAA claim fails for a second, independent reason: they have not adequately alleged "loss" as required by the statute. "Under the CFAA, Plaintiffs must also plead that [defendants'] actions caused loss of more than \$5,000 during any one-year period." *Brodsky*, 2019 WL 4141936, at *7; *see also* 18 U.S.C. § 1030(c)(4)(A)(i)(I). The statute defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." 18 U.S.C. § 1030(e)(11). The statutory definition of "loss" "focus[es] on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data." *Van Buren*, 593 U.S. at 392.

Plaintiffs offer three theories of loss. First, they point to the "secret transmission of ... [their] private and personally identifiable data and content," which "caused a diminution in value of ... [their] personal information." [22] ¶ 158. Second, they allege that the transmission of their data "frequently and systematically drained ... [their] devices and batteries." *Id.* Third, they allege that "Defendants' unauthorized access to Plaintiffs' devices requires evaluation by professionals to determine potential remedial measures." *Id.*

As for the diminution of value of plaintiffs' data, the Court follows the lead of other courts that have held this type of loss is not cognizable under the CFAA. In

Andrews v. Sirius XM Radio Inc., 932 F.3d 1253 (9th Cir. 2019), plaintiff similarly asserted loss based on the diminished value of his personal information and his inability to commodify it in the future. *Id.* at 1262. The Ninth Circuit observed that the “statute’s ‘loss’ definition—with its references to damage assessments, data restoration, and interruption of service—clearly limits its focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself.” *Id.* at 1263. Because this “narrow conception of loss” did not align with plaintiff’s theory of diminution of value, *Andrews* concluded that the plaintiff could not state a CFAA claim. *Id.*; *see also Cottle*, 536 F. Supp. 3d at 486 (applying *Andrews* to reject a similar theory of CFAA loss).

Plaintiffs’ theory of loss related to battery drainage is also defective. Plaintiffs do not allege their battery drain was at least \$5,000 during any one-year period or explain how to value battery drain at all. The parties dispute whether the class may aggregate damages to reach the \$5,000 CFAA minimum, but that dispute makes no difference where plaintiffs have not attempted—individually or as a class—to show their work. *See Ji v. Naver Corp.*, No. 21-CV-05143-HSG, 2023 WL 6466211, at *11 (N.D. Cal. Oct. 3, 2023) (“Even assuming there are millions of people in the class, Plaintiffs fail to plead any facts regarding how to monetarily value battery drain so as to satisfy the \$5,000 annual requirement.”); *cf. Brodsky*, 2019 WL 4141936, at *8 (“Plaintiffs’ bald assertion of \$5,000 in damages based on 2-5 minute login delays without any facts to support the allegation is ‘insufficient to sustain a CFAA claim.’”).

Plaintiffs’ claim that their devices required “evaluation by professionals” is similarly speculative without some indication that plaintiffs *actually* consulted professionals in response to defendants’ alleged unauthorized access and paid at least \$5,000 per year for those services. The complaint only vaguely alleges that “Defendants’ unauthorized access to Plaintiffs’ devices *requires* evaluation by professionals to determine potential remedial measures.” *See id.* ¶ 158 (emphasis added). As is, this allegation is not “enough to raise a right to relief above the speculative level.” *Twombly*, 550 U.S. at 555.

On these grounds, Count I is dismissed without prejudice.

C. Computer Data Access and Fraud Act (Count V)

Plaintiffs bring suit under § 502(c)(1) and (2) of the Computer Data Access and Fraud Act (“CDAFA”). Section 502(c)(1) punishes an entity that “[k]nowingly 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.” 18 U.S.C. § 502(c)(1). Meanwhile, § 502(c)(2) punishes an entity that “knowingly accesses and without permission takes, copies, or makes use of any data from a computer.” *Id.* § 502(c)(2).

To state a claim under the CDAFA, plaintiffs must allege a cognizable loss. “In the context of a § 502 violation, ‘loss’ has been defined to encompass costs related to fixing a computer, lost revenue, or other consequential damages incurred due to an interruption of computer services.” *Pratt v. Higgins*, No. 22-CV-04228-HSG, 2023 WL

4564551, at *9 (N.D. Cal. July 17, 2023). This narrow definition of “loss” is understood to encompass specific harms related to computer intrusions, not broader losses based on the eventual sharing of data with third parties. *Id.* at *9. Plaintiffs do not articulate any theories of loss for their CDAFA claim different than the theories of loss already discussed in connection with their CFAA claim. *See generally* [22] ¶¶ 219–22. For those same reasons, none of plaintiffs’ theories of harm are cognizable under the CDAFA.

Count V is dismissed without prejudice.

D. Video Privacy Protection Act (Count II)

The Video Privacy Protection Act (“VPPA”) provides that a “video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person.” 18 U.S.C. § 2710(b)(1). But CapCut is not a “video tape service provider” within the meaning of the statute, and so plaintiffs’ VPPA claim fails.

Under the VPPA, a “video tape service provider” is “any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials.” 18 U.S.C. § 2710(a)(4). Based on the plain language of this statute and according to plaintiffs’ own complaint, CapCut is not a “video tape service provider.” Unlike Blockbuster, Hollywood Video, and even more modern services like Netflix, Hulu, and Amazon Prime, CapCut is not “engaged in the business” of renting, selling, or even delivering audio visual *materials*. Rather, CapCut provides users with a *service*. It is a video-

editing application, which, as plaintiffs allege, “allows users to create, edit and customize videos” using “various templates, filters, visual effects, and music.” [22] ¶ 1. As defendants put it: “Users provide their videos to CapCut, not the other way around.” [31] at 11.

Plaintiffs attempt to sidestep this issue in two ways. First, they contend that CapCut “delivers” video content to users because it “offers users a library of copyright-free media assets, including stock videos.” [36] at 17 (quoting [22] ¶ 62). But the mere act of making stock videos and templates available for use in video projects does not mean that CapCut is engaged *in the business of* delivering videos. *See In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1221 (C.D. Cal. 2017) (“‘Business’ connotes ‘a particular field of endeavor,’ *i.e.*, a focus of the defendant’s work.”) (quoting Webster’s Third New International Dictionary 302 (1981) (def. 1d)). The focus of CapCut’s “business” is to serve as a video-editing application, and providing stock videos and templates is an ancillary part of that business model. That much is clear from plaintiffs’ complaint, which repeatedly describes CapCut as a “video editor” or an app that allows users “to create and edit videos.” *E.g.*, [22] ¶¶ 1, 3, 48–51, 53, 55–56, 60–61. By comparison, any mention of CapCut’s media library in the complaint is limited to two non-conclusory paragraphs and even those paragraphs make clear the library’s role is to help CapCut users with their video-editing projects. *Id.* ¶¶ 62–63.

Second, plaintiffs contend that CapCut delivers videos because users are provided “a unique edited video that users did not previously possess.” [36] at 17. To

support a broad reading of “deliver,” plaintiffs point to § 2710(a)(3), which defines PII as information identifying a person as having requested “video materials *or services*.” 18 U.S.C. § 2710(a)(3) (emphasis added). But the relevant question is the definition of “video tape service provider” in § 2710(a)(4), not the definition of PII in § 2710(a)(3), and the former definition limits “video tape service provider” to those who deliver “prerecorded video cassette tapes or similar audio visual *materials*,” not “services.” *Id.* § 2710(a)(4) (emphasis added).⁴

Because further amendment would be futile with respect to plaintiffs’ VPPA claim, Count II is dismissed with prejudice. *See Esco v. City of Chicago*, 107 F.4th 673, 683 (7th Cir. 2024).

E. Electronic Communications Privacy Act & California Invasion of Privacy Act (Counts III & X)

The Electronic Communications Privacy Act of 1986 (“ECPA”) prohibits the unauthorized “interception” of an “electronic communication.” 18 U.S.C. § 2511(1)(a)–(e). The ECPA defines “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). In much the same way, the California Invasion of Privacy Act (“CIPA”) prohibits any person from using electronic

⁴ To be sure, the definition of “video tape service provider” could encompass more modern means of delivering audio visual materials, such as online applications and streaming services. *See* [36] at 16–17; *see also In re Hulu Privacy Litig.*, No. C 11–03764 LB, 2012 WL 3282960, at *5 (N.D. Cal. Aug. 10, 2012) (definition of “video tape service provider” is about “the video content, not about how that content was delivered (e.g. via the Internet or a bricks-and-mortar store)”). But as a video-editing service rather than a supplier of materials, CapCut falls outside even that more expansive understanding of what constitutes a “video tape service provider.”

means to “learn the contents or meaning” of any “communication” “without consent” or in an “unauthorized manner.” Cal. Pen. Code § 631(a).

Neither the ECPA nor CIPA imposes liability on a person who is a “party” to the communication. *Id.* § 2511(2)(d) (“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”); *Warden v. Kahn*, 99 Cal. App. 3d 805, 811 (1979) (“[S]ection 631 ... has been held to apply only to eavesdropping by a third party and not to recording by a participant to a conversation.”). “[T]he relevant inquiry is whether the defendant is a participant in the conversation, as opposed to a non-participant that uses other means to gain access to—*i.e.*, intercept—the communication.” *Zak v. Bose Corp.*, No. 17-CV-02928, 2019 WL 1437909, at *3 (N.D. Ill. Mar. 31, 2019) (citing *United States v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964)).

In their response, plaintiffs posit that defendants intercepted their data—thus exempting them from the party exception to liability—by “redirect[ing]” the contents of their communications “to third parties, including the CCP, who were not authorized to have them.” [36] at 19. To support this argument, plaintiffs point to several cases where defendants installed tracking software on their websites and then shared the information they collected with third parties. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 596, 607–08 (9th Cir. 2020) (“*Facebook Tracking*”) (plaintiff stated claim against Facebook where the website used a plug-in to track user browsing histories and sold the data to advertisers); *Saleh v. Nike, Inc.*,

562 F. Supp. 3d 503, 519–21 (C.D. Cal. 2021) (plaintiffs stated claim where Nike embedded software into website that allowed third party to capture data); *Kauffman v. Papa John’s Int’l, Inc.*, No. 22-CV-1492-L-MSB, 2024 WL 171363, at *1, *7 (S.D. Cal. Jan. 12, 2024) (Papa John’s not subject to party exception where it installed software enabling it and a third party to track plaintiffs’ interactions with the Papa John’s website).

There are at least two problems with plaintiffs’ “redirected data” argument. First, based on plaintiffs’ allegations, it is not clear whether any communications were intercepted while in transit as opposed to merely shared with third parties after the fact. Although the Seventh Circuit has declined to decide whether the interception must be contemporaneous with transmission, *see Epstein v. Epstein*, 843 F.3d 1147, 1149–51 (7th Cir. 2016); *United States v. Szymuszkiewicz*, 622 F.3d 701, 705–06 (7th Cir. 2010), “[e]very court of appeals to consider the issue” has reached this conclusion. *See Peters v. Mundelein Consol. High Sch. Dist. No. 120*, No. 21 C 0336, 2022 WL 393572, at *11 (N.D. Ill. Feb. 9, 2022) (citing *Boudreau v. Lussier*, 901 F.3d 65, 77 (1st Cir. 2018)). True, plaintiffs assert in their complaint that defendants “intercept” plaintiffs’ communications, *see id.* ¶¶ 184, 186–91, 270, but these allegations are purely conclusory. Without additional support, and even viewing this allegation in the light most favorable to plaintiffs, the Court cannot reasonably infer that the communications were intercepted in real-time. This is especially true where the complaint otherwise alleges only that the CCP “is able to *access* international and US

data,” *id.* ¶ 76 (emphasis added), and that ByteDance was “monitored by a special committee of [CCP] members,” *id.* ¶ 77.

Second, plaintiffs’ allegations fall short of the software-tracking devices that proved sufficient to state a claim in their cited authority. In *Facebook Tracking*, plaintiffs alleged a scheme by which Facebook installed a plug-in that “continued to collect their data after they had logged off the social media platform, in order to receive and compile their personally identifiable browsing history.” 956 F.3d at 598. In that case, the communications were between the user and the third-party website. *Id.* at 608. So when Facebook’s plug-in directed the website to duplicate browsing history and send it to Facebook, the party exception did not “exempt [Facebook] from liability.” *Id.*; *see also Szymuszkiewicz*, 622 F.3d at 705–06 (defendant who installed a software to forward emails to his own account contemporaneously could be liable under the ECPA); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 840 (N.D. Cal. 2014) (plaintiffs plausibly alleged interception where they alleged Facebook used software that scanned URLs contained in users’ messages and then used that information for targeted advertising and to gather “likes” for those URLs). Unlike in these cases, plaintiffs here do not allege any specific mechanism by which defendants contemporaneously redirected their communications to third parties.

In addition to § 631, plaintiffs also bring a claim under § 632 of the CIPA, which imposes liability on any party who “uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication.” Cal. Pen. Code § 632(a). But beyond a conclusory statement that “[d]efendants intercepted and

recorded videos” without “the consent of either the sender or recipient,” plaintiffs do not allege that defendants used (1) an electronic amplifying device or (2) a recording device to eavesdrop on plaintiffs’ conversations. Plaintiffs’ conclusory allegations of “eavesdropping” and “recording” thus lack sufficient detail. *See* [36] at 22 (citing [22] ¶¶ 75–78, 270).

Counts III and X therefore are dismissed without prejudice.

F. Stored Communications Act (Count IV)

Plaintiffs also bring claims under § 2702(a)(1) and (2) of the Stored Communications Act (“SCA”). Section 2702(a)(1) provides that “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1). Section 2702(a)(2) similarly prohibits entities that provide “remote computing service to the public” from knowingly divulging the contents of communications. *Id.* § 2702(a)(2). Plaintiffs allege that defendants violated the SCA when they divulged the contents of their information to unauthorized parties, including the CCP. [22] ¶ 209. But in their current iteration, plaintiffs’ allegations are not “enough to raise a right to relief above the speculative level.” *Twombly*, 550 U.S. at 555; *see also* [31] at 18.

To support their claims of disclosed data, plaintiffs reference a June 2022 BuzzFeed News article that cites leaked audio from company employees, which plaintiffs say demonstrates that “China-based ByteDance has repeatedly accessed non-public data of U.S. TikTok users.” [22] ¶ 75. As a preliminary matter, this article

relates to the disclosure of data from TikTok, not CapCut. And unlike TikTok (which is run by a separate entity in the United States, *id.* ¶ 29), plaintiffs themselves acknowledge that CapCut is run directly by ByteDance. *See* [22] ¶¶ 31, 48. Therefore, based on the allegations in the complaint, the Court cannot reasonably infer that any disclosure of data collected via CapCut to ByteDance would have been unauthorized.

Plaintiffs also cite public statements from a former head of engineering for ByteDance’s U.S. operations who said the CCP “had its own office where it would access all ByteDance data.” [22] ¶ 76. The former ByteDance employee also said in a sworn declaration that a special committee of CCP members had a “super user credential” enabling them to “view all the data collected by ByteDance, including U.S.-based user data.” *Id.* ¶ 77. These statements are not enough to state a plausible claim for relief. They do not establish that the CCP had access to user communications, as opposed to user data. *See* 18 U.S.C. § 2702(a)(1) (imposing liability only when an entity knowingly divulges the “contents of a *communication*”) (emphasis added). The article plaintiffs cite says the engineer was terminated in 2018, which was well before CapCut ever launched in the United States.⁵ *See* Hannah Rooke, *TikTok Insider Says Chinese Government Has Backdoor to User Data*, YAHOO.COM (May 17, 2023), <https://www.yahoo.com/lifestyle/tiktok-insider-says-chinese-government-093502126.html>; [22] ¶ 48. So even if ByteDance shared user

⁵ The Court takes judicial notice of this article as it is incorporated into the complaint by reference. *See Tellabs, Inc. v. Makor Issues & Rts., Ltd.*, 551 U.S. 308, 322 (2007) (“[C]ourts must consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference.”); *see also* 5B Wright & Miller § 1357 (4th ed.) (2024).

communications with the CCP in 2018, it is too much to presume based on the engineer's statement that these activities were ongoing several years later when CapCut became available to users in the United States.

Plaintiffs also allege a violation of § 2701(a), which punishes whoever “intentionally accesses without authorization a facility through which an electronic communication service is provided.” 18 U.S.C. § 2701(a)(1). But as defendants point out, § 2701(a)'s prohibition does not apply to the “entity providing a wire or electronic communications service,” *id.* § 2701(c)(1), and plaintiffs' complaint squarely admits that “[d]efendants provide an electronic communication service within the meaning of the SCA.” [22] ¶ 199. So long as plaintiffs admit they provide an “electronic communication service,” their § 2701(a) claim cannot stand.

Count IV is dismissed without prejudice.

G. Constitutional and Common-Law Privacy Claims (Counts VI and VII)

Plaintiffs next raise claims for violations of their right to privacy under the California Constitution and intrusion upon seclusion under California's common law. California courts condense both these causes of action into a single analysis that considers: “(1) whether there is a reasonable expectation of privacy, and (2) whether the intrusion was highly offensive.” *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1088 (N.D. Cal. 2022). “A reasonable expectation of privacy can exist where a defendant gains ‘unwanted access to data by electronic or other covert means, in violation of the law or social norms.’” *Id.* (quoting *Facebook Tracking*, 956 F.3d at 601–02). “Courts consider the customs, practices, and circumstances surrounding the

data collection, including the amount of data collected, the sensitivity of data collected, the manner of data collection, and the defendant's representations to its customers." *Id.* (citing *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal.4th 1, 36 (1994)).

Defendants first argue that plaintiffs cannot state a claim under either theory because they consented to the data collection via CapCut's Terms of Service or Privacy Policy. But, as already discussed, whether plaintiffs consented to the data collection is a question of fact not amenable to resolution on the present record. *See supra* at 5–8.

With the consent issue aside, the Court considers whether plaintiffs have stated a claim as to the collection of each type of private data defendants allegedly collected: videos and images; user identifiers, registration information, and sign-up information; location information; and biometric information. To the extent defendants argue that "common sense" dispels plaintiffs' reasonable expectation of privacy in the collection of their data, the Court views this contention as part and parcel with whether plaintiffs' expectation of privacy was objectively "reasonable" and considers it as part of the discussion that follows.

Beginning with the collection of videos and images, defendants contend that "there must be something sensitive about those videos [and images] that creates a reasonable expectation of privacy in them." [31] at 20. Because the California plaintiffs do not allege their photos and videos were "sensitive or private in any way," defendants say they cannot serve as the basis of a privacy claim. *Id.* at 21. However, the right to privacy does not depend solely on the sensitivity of the particular content

collected but also considers whether “the *manner* it was collected ... violate[d] social norms.” *Facebook Tracking*, 956 F.3d at 603 (emphasis added). In *Facebook Tracking*, for example, plaintiffs alleged that Facebook collected full-string detailed URLs from websites that plaintiffs visited even after they had logged out of the Facebook application. *Id.* at 603, 605. In concluding that plaintiffs had adequately alleged an expectation of privacy, the appeals court did not evaluate the specific content of the URLs that Facebook collected but instead focused on the fact that users would not expect Facebook to collect information about their habits on third-party websites when they were not operating within Facebook itself. *Id.* at 603–04.

Here, like in *Facebook Tracking*, plaintiffs challenge the manner in which data was collected. Specifically, they allege that CapCut accesses and collects *all* the videos and photos stored on their devices, not just those they voluntarily uploaded to the CapCut app. *See* [22] ¶ 11 (alleging that, with regard to plaintiff Rodriguez, “the CapCut app gained access to all of the photos and videos on her device”); *id.* ¶ 120 (alleging that defendants “took plaintiffs’ ... private videos and audio-visual material from their devices”). Taking these allegations as true, plaintiffs have sufficiently alleged a reasonable expectation of privacy in this data. When using a video-editing app, a reasonable CapCut user would not expect the app to access and collect all the photos and videos on their devices, regardless of whether they use those photos and videos to create content within the app. *Cf. Riley v. California*, 573 U.S. 373, 397–99 (2014) (recognizing that individuals have a reasonable expectation of privacy in the contents of their cell phones due to the large amount of personal data stored

therein); *Hibbert v. Schmitz*, No. 16-CV-3028, 2019 WL 8405217, at *16 (C.D. Ill. Feb. 7, 2019) (plaintiff’s expectation of privacy “in her phone and its contents is one that society is prepared to recognize as reasonable”). The proffered nature and scope of this alleged practice is enough at this early stage. *See Narducci v. Moore*, 572 F.3d 313, 320 (7th Cir. 2009) (taking facts in light most favorable to plaintiff, he demonstrated a reasonable expectation of privacy in phone line at work).

As for the user/device identifiers, registration information, and sign-up information, courts have held that there is no reasonable expectation of privacy in these types of data. *See, e.g., Ji v. Naver Corp.*, No. 21-CV-05143-HSG, 2022 WL 4624898, at *7 (N.D. Cal. Sept. 30, 2022) (“Plaintiffs have not alleged enough facts to show that the ‘user and device identifiers’ are the type of information that could give rise to a privacy injury.”); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) (“[T]he Court is hard pressed to conclude that basic contact information, including one’s email address, phone number, or Facebook or Zynga username, is private information.”). Nothing about the allegations here compels a different conclusion; there can be no objectively reasonable expectation of privacy in the type of information that users knowingly provided when signing up for CapCut’s services. *See generally United States v. Soybel*, 13 F.4th 584, 590–91 (7th Cir. 2021) (“A person generally ‘has no legitimate expectation of privacy in information he voluntarily turns over to third parties,’ subjective expectations notwithstanding.”) (quoting *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979), and also citing *United States v. Miller*, 425 U.S. 435, 442 (1976)).

Next up is the collection of plaintiffs' location data. Defendants do not argue that plaintiffs lack a reasonable expectation of privacy in their location information; they only argue that plaintiffs consented to the collection of such data. As discussed, whether plaintiffs consented to their data is a factual question to be determined at a later stage in the litigation.

Defendants also argue generally that plaintiffs "do not allege a highly offensive intrusion." [38] at 14. "Determining whether a defendant's actions were 'highly offensive to a reasonable person' requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *Facebook Tracking*, 956 F.3d at 606. Without further briefing from the parties on these issues, the Court is not prepared to hold, as a matter of law, that no reasonable person would find the collection of "fine-grained location information" to be highly offensive. Indeed, depending on the duration of the collection, such a conclusion could be in tension with *Carpenter v. United States*, 585 U.S. 296, 311 (2018) (concluding that defendant had a reasonable expectation of privacy under the Fourth Amendment in historical cell-site records tracking his location for 127 days). At this juncture, the Court therefore concludes that plaintiffs may proceed with their constitutional and common-law privacy claims based on the collection of their location data. *See Rivera v. Google, Inc.*, 366 F. Supp. 3d 998, 1012 (N.D. Ill. 2018) (finding plaintiffs had a reasonable expectation of privacy in Google's collection of their location data).

Finally, regarding biometric data, defendants do not contend that plaintiffs lack a reasonable expectation of privacy in that collection. Instead, they argue that plaintiffs “do not adequately allege that any biometric identifiers were collected from them” at all. [31] at 20. For the reasons discussed in more detail later in this opinion, *see infra* at 39–43, the Court finds that plaintiffs have adequately alleged the collection of their biometric data. And, like the location data, it suffices for now to say that a reasonable person could find the collection of face scans and voiceprints to be highly offensive. *See Naver*, 2022 WL 4624898, at *10 (plaintiffs stated intrusion upon seclusion and California constitutional privacy claims based on collection of their biometric information). Therefore, plaintiffs may also proceed at this juncture with their constitutional and common-law privacy claims based on the collection of their biometric data.

In sum, plaintiffs may proceed with their constitutional and common-law privacy claims based on the collection of their photos and videos, location data, and biometric data. To the extent plaintiffs bring these claims based on the collection of user identifiers, registration information, and sign-up information, plaintiffs’ claims are dismissed without prejudice.

H. Unfair Competition Law (Count VIII)

Plaintiffs next allege that defendants violated California’s Unfair Competition Law (“UCL”), which prohibits any “unlawful, unfair or fraudulent business act or practice.” Cal. Bus. & Prof. Code § 17200. Because a UCL claim “sound[s] in fraud,” plaintiffs “must state with particularity the circumstances constituting fraud”

pursuant to Rule 9(b). *Elias v. Hewlett-Packard Co.*, 903 F. Supp. 2d 843, 853 (N.D. Cal. 2012); Fed. R. Civ. P. 9(b).

A plaintiff has statutory standing to sue under the UCL only if they “lost money or property as a result of the unfair competition.” Cal. Bus. & Prof. Code § 17204. “[A] plaintiff ... must demonstrate some form of economic injury.” *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 323 (2011). The requirement “confine[s] standing to those actually injured by a defendant’s business practices and [] curtail[s] the prior practice of filing suits on behalf of clients who have not used the defendant’s product or service, viewed the defendant’s advertising, or had any other business dealing with the defendant.” *Id.* at 321. Plaintiffs offer four theories to satisfy this requirement: (1) the diminution in the value of their data, (2) that their devices have “been impaired and slowed,” (3) that they incurred data and electricity costs, and (4) that they were harmed by the invasion of their privacy. [22] ¶ 254. None of these four theories suffices to establish that plaintiffs “lost money or property as a result of” defendants’ data privacy practices. Cal. Bus. & Prof. Code § 17200.

Beginning with the first theory, based on the complaint before it, plaintiffs’ allegations do not meet the heightened requirements under Rule 9(b). Even if the diminution in value of plaintiffs’ data could constitute an economic loss, plaintiffs do not allege that they have tried to sell their data and have received a lesser price for it. *See Griffith*, 2023 WL 9019035, at *6 (plaintiffs had not stated a UCL claim because they failed to allege the surveys they wished to participate in “either declined to let them participate ... or paid them less than they would have otherwise

received”). Nor do they allege that they even *intended* to sell their data on the personal-data market. *See In re Meta Pixel*, 724 F. Supp. 3d at 1024 (plaintiffs could support UCL standing if they alleged they “attempted or intended to participate in the market for their data”) (cleaned up). Plaintiffs also have “not shown how this information has economic value to [them].” *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) (“That the information has external value, but no economic value to plaintiff, cannot serve to establish that plaintiff has personally lost money or property.”). Without plausible allegations that plaintiffs *themselves* planned to “derive economic value from their PII,” on this record plaintiffs cannot establish that they in fact “lost money or property” according to the diminished-value theory. *Id.* (quoting *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 538 (2022)).⁶

Plaintiffs’ citation to *Facebook Tracking* does not persuade the Court otherwise. 956 F.3d at 600. That case did not consider whether the diminished-value theory was sufficient to establish statutory standing to sue under the UCL—it only considered whether it was sufficient to confer standing under Article III. *Id.* at 600; *Griffith*, 697 F. Supp. 3d at 977 (declining to rely on *Facebook Tracking* because it only dealt with Article III standing); *Hazel v. Prudential Fin., Inc.*, No. 22-CV-07465, 2023 WL 3933073, at *6 (N.D. Cal. June 9, 2023) (same). And the UCL’s standing requirement is “substantially narrower than federal standing” under Article III. *See Kwikset*, 51 Cal.4th at 324. “Whereas a federal plaintiff’s injury in fact may be

⁶ Because plaintiffs have not adequately alleged that their data lost value, any theory that they were deprived the “benefit of their bargain” when they paid to access CapCut’s additional features also falls short.

intangible and need not involve lost money or property, ... [the UCL requires] that a plaintiff's injury in fact specifically involve lost money or property.” *Id.* (cleaned up).

Plaintiffs’ remaining theories of economic loss fare no better. Besides the conclusory statements that the “battery, memory, CPU and bandwidth of [their] devices have been compromised” and “they have incurred additional data usage and electricity costs,” plaintiffs offer no details to support their second and third theories of loss. [22] ¶ 254. These allegations therefore fall short of Rule 9(b)’s particularity requirement. *See Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1056 (N.D. Cal. 2014) (“Because Plaintiffs have not quantified or otherwise articulated the alleged resource usage, they fail to allege an injury that can serve as the basis of standing.”). As for their final theory, plaintiffs have offered no explanation why they experienced actual loss from the invasion of their privacy.⁷

Count VIII is dismissed without prejudice.

I. False Advertising Law (Count IX)

Plaintiffs next bring a claim under California’s False Advertising Law (“FAL”), which “makes it unlawful for a business to disseminate any statement ‘which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading.’” *Elias*, 903 F. Supp. 2d at 853 (quoting Cal. Bus. & Prof. Code § 17500). “Whether an advertisement is ‘misleading’ must be judged by the effect it would have on a reasonable consumer.” *Id.* (citing *Williams v.*

⁷ Because the Court finds that plaintiffs have not adequately alleged standing under the UCL, it need not reach defendants’ argument that plaintiffs have not adequately alleged an unlawful, unfair, or fraudulent business practice.

Gerber Products Co., 552 F.3d 934, 938 (9th Cir. 2008)). Like their UCL claim, plaintiffs must also meet Rule 9(b)’s heightened pleading requirement. *Id.*; Fed. R. Civ. P. 9(b).

Here, plaintiffs base their FAL claim on defendants’ alleged failure to disclose the collection of their private information and its sharing of the data with the CCP and foreign government entities. [22] ¶ 259. Plaintiffs also allege that “[d]efendants’ advertising and other statements regarding CapCut are, and at all relevant times were, highly misleading.” *Id.*

FAL claims are subject to the same economic loss requirement as claims brought under the UCL. *See In re Ferrero Litig.*, 794 F. Supp. 2d 1107, 1111 (S.D. Cal. 2011) (“In order to assert a claim under the UCL or FAL, a person must have ‘suffered injury in fact and ha[ve] lost money or property.’”) (quoting Cal. Bus. & Prof. Code § 17535). Thus, for the same reasons just discussed, plaintiffs cannot establish they have statutory standing to bring a claim under the FAL.

Moreover, to state a claim under the FAL, a plaintiff must have experienced an economic injury “as a result of [defendants’] unfair competition.” *Id.* (quoting Cal. Bus. & Prof. Code § 17535). In other words, “actual reliance is required to have standing to sue under the ... FAL.” *Id.* In this case, plaintiffs do not allege that they relied on defendants’ alleged misrepresentations when deciding whether to use CapCut’s services, and their conclusory allegation that they “have been harmed and have suffered economic injury *as a result of* Defendants’ misrepresentations” does not suffice under Rule 9(b). [22] ¶ 261 (emphasis added); *see also Hammerling*, 615 F.

Supp. 3d at 1081 (plaintiffs’ statement that they would not have purchased their Android smartphones had they known Google would collect their data was not enough to plead reliance).⁸

To the extent plaintiffs’ FAL claim relies on an omission, their allegations also fall short. “To plausibly allege a fraudulent omission, the omission must either (1) ‘be contrary to a representation actually made by the defendant,’ or (2) ‘an omission of a fact the defendant was obliged to disclose.’” *Rodriguez v. Mondelez Glob. LLC*, 703 F. Supp. 3d 1191, 1209 (S.D. Cal. 2023) (quoting *Hodsdon v. Mars, Inc.*, 891 F.3d 857, 865 (9th Cir. 2018)). Plaintiffs have not pointed to any contrary representation, nor have they alleged why defendants were obligated to disclose their data-collection practices other than to assert in a conclusory manner that they “were under a duty to disclose” based on their contractual relationship with plaintiffs.⁹ See [22] ¶¶ 119, 253; *see also Hammerling*, 615 F.Supp.3d at 1081 (“The fraudulent omission claims fail because Google lacked a duty to disclose its data collection practices.”).

Count IX is dismissed without prejudice.

⁸ In a footnote of their response brief, plaintiffs point to one alleged affirmative misrepresentation on CapCut’s website, which read as follows: “Bring privacy and security into your life with CapCut’s free cloud storage. Simply make your account, and rest assured that your data will remain safe whenever you return.” [36] at 30 n.27 (citing [22] ¶ 65). But plaintiffs do not allege that they actually relied on this alleged misrepresentation. See *In re Ferrero Litig.*, 794 F. Supp. 2d at 1111.

⁹ Although the “law concerning a defendant’s duty to disclose in a fraudulent omissions case is ‘marked by general disarray,’” *Hammerling* laid out two tests used to determine whether a defendant has a duty to disclose. *Hammerling*, 615 F.Supp.3d at 1085 (quoting *In re Toyota RAV4 Hybrid Fuel Tank Litig.*, 534 F. Supp. 3d 1067, 1101 (N.D. Cal. 2021)). At this stage in the litigation, plaintiffs have not established that they meet either of these two tests.

J. Larceny and Conversion (Counts XI & XII)

Plaintiffs next raise claims for common law larceny and conversion. “California Penal Code Section 484 forbids theft, which includes obtaining property ‘by ... false ... representation or pretense.’” *Calhoun*, 526 F. Supp. 3d at 635 (quoting Cal. Penal Code § 484). In addition, “California Penal Code Section 496(a) prohibits the obtaining of property ‘in any manner constituting theft.’” *Id.* (quoting Cal. Penal Code § 496(a)). A plaintiff states a claim for conversion if they plausibly allege: “(1) the plaintiff’s ownership or right to possession of the property; (2) the defendant’s conversion by a wrongful act or disposition of property rights; and (3) damages.” *Lee v. Hanley*, 61 Cal. 4th 1225, 1240 (2015).

Defendants make a compelling argument that they could not have stolen or converted plaintiffs’ videos to the extent plaintiffs willingly housed them within the CapCut platform and on CapCut’s servers. *See Best Carpet Values, Inc. v. Google, LLC*, 90 F.4th 962, 969 (9th Cir. 2024) (a website copy is not “capable of exclusive possession or control” because plaintiffs did not “retain control over the copies of their websites that are generated and sent to users’ devices”); *Snapkeys, Ltd. v. Google LLC*, 539 F. Supp. 3d 1040, 1056 (N.D. Cal. 2021) (no conversion where plaintiffs gave smartwatches to Google as product samples). But, as discussed, plaintiffs also allege that defendants collected videos from their devices that they did not willingly provide to CapCut. *See supra* at 25–26. In any case, plaintiffs allege more than the theft or conversion of their videos; they also claim that defendants unlawfully collected their “personal information and private data.” [22] ¶¶ 283, 288. Other parts of the

complaint make clear that this data was not limited to videos but also included phone and social network contacts, location data, and product interaction and user data. *Id.* ¶ 103. Even more so, in some cases (such as the collection of location data), plaintiffs allege that they did not know that data was being collected at all. *See* [22] ¶ 100 (“[U]nbeknownst to users,” defendants collected plaintiffs’ “private and personally identifiable data and content.”) (emphasis added).

As for these other data, defendants cite to *Low* to argue that personal data is generally not considered property. [31] at 25 n.8 (citing *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1030 (N.D. Cal. 2012)). True, the court in *Low* commented in 2012 that “the weight of authority holds that a plaintiff’s ‘personal information’ does not constitute property.” 900 F. Supp. 2d at 1030. But even the judge in *Low* has since acknowledged that the “growing trend across courts ... [is now] to recognize the lost property value” of personal information. *Calhoun*, 526 F. Supp. 3d at 635 (quoting *In re Marriott Int’l, Inc. Cust. Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020)); *see also Griffith*, 697 F. Supp. 3d at 976 (agreeing with *Calhoun* that plaintiffs can have a property interest in their personal data). The Court follows the prevailing trend to allow plaintiffs’ property claims based on the alleged theft and conversion of their personal data.

Defendants have not offered any other grounds to dismiss plaintiffs’ claims for larceny and conversion. The Court therefore denies the motion to dismiss as to Counts XI & XII.

K. Restitution and Unjust Enrichment (Count XIII)

To allege unjust enrichment, “a plaintiff must show that a defendant received and unjustly retained a benefit at the plaintiff’s expense.” *Russell v. Walmart, Inc.*, 680 F. Supp. 3d 1130, 1133 (N.D. Cal. 2023) (quoting *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016)). “[R]estitution generally requires that a defendant has been unjustly conferred a benefit through mistake, fraud, coercion, or request.” *Id.* (quoting *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015)). In California, “there is not a standalone cause of action for unjust enrichment.” *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015) (cleaned up). However, “[w]hen a plaintiff alleges unjust enrichment, a court may ‘construe the cause of action as a quasi-contract claim seeking restitution.’” *Hammerling*, 615 F. Supp. 3d at 1096 (quoting *Astiana*, 783 F.3d at 762).

It is “well settled that an action based on an implied-in-fact or quasi-contract cannot lie where there exists between the parties a valid express contract covering the same subject matter.” *O’Connor v. Uber Techs., Inc.*, 58 F. Supp. 3d 989, 999–1000 (N.D. Cal. 2014) (quoting *iLance Camper Mfg. Corp. v. Republic Indem. Co.*, 44 Cal.App.4th 194, 203 (2d Dist. 1996)). Relying on this principle, defendants maintain that the unjust enrichment claim fails because plaintiffs entered into an express contract with defendants via CapCut’s Terms of Service. [31] at 26. But as discussed earlier, factual issues remain as to whether plaintiffs ever agreed to any Terms of Service and, if so, which version of the Terms they agreed to. *See supra* at 5–8. On

this record, dismissal of plaintiffs’ unjust enrichment claim based on CapCut’s Terms of Service would be improper.

Citing the Ninth Circuit’s decision in *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844–45 (9th Cir. 2020), defendants also argue that plaintiffs cannot state a claim for unjust enrichment because plaintiffs “have an adequate legal remedy” and “allege the exact same conduct” under other causes of action seeking damages. [31] at 26. Plaintiffs counter they have alleged that legal remedies are inadequate and no more is required to survive a motion to dismiss. [36] at 31; [22] ¶ 256 (“California Plaintiffs and the California Subclass lack an adequate remedy at law and thus are entitled to seek equitable relief.”).

In *Sonner*, a consumer plaintiff brought a putative class action against a dietary supplement maker, seeking both damages and equitable restitution for false and misleading advertising under the UCL and California’s Consumer Legal Remedies Act (“CLRA”). 971 F.3d 834 at 838. The plaintiff amended the complaint to drop the CLRA damages claim on the eve of trial; the district court granted defendant’s motion to dismiss and denied plaintiff leave to amend the complaint to re-allege the CLRA damages claim. *Id.* at 837. On appeal, the Ninth Circuit held that the plaintiff was not entitled to unjust enrichment for violating the UCL and CLRA because she did “not allege that [she] lack[ed] an adequate legal remedy.” *Id.* at 844. The appeals court emphasized that plaintiff sought “the same sum in equitable restitution as a full refund of the purchase price—\$32,000,000—as she requested in damages to compensate her for the same past harm.” *Id.*

District courts have understood *Sonner* to teach “that a plaintiff, on the eve of trial, cannot create an inadequacy of a legal remedy by eliminating its availability by taking volitional action.” *E.g., Nacarino v. Chobani, LLC*, 668 F. Supp. 3d 881, 895 (N.D. Cal. 2022). However, “*Sonner* has limited applicability to the pleading stage.” *Jeong v. Nexo Fin. LLC*, No. 21-CV-02392-BLF, 2022 WL 174236, at *27 (N.D. Cal. Jan. 19, 2022); *see also Johnson v. Trumpet Behav. Health, LLC*, No. 3:21-CV-03221-WHO, 2022 WL 74163, at *3 (N.D. Cal. Jan. 7, 2022) (“[I]f a plaintiff pleads that she lacks an adequate legal remedy, *Sonner* will rarely (if ever) require more this early in the case.”); *In re JUUL Labs, Inc., Mktg., Sales Pracs., & Prods. Liab. Litig.*, 497 F. Supp. 3d 552, 638 (N.D. Cal. 2020) (“The facts of *Sonner* ... are inapposite considering the allegations and the posture of the [complaint].”). This approach, as other courts have noted, is “consistent with Federal Rule of Civil Procedure 8 which allows for pleading in the alternative.” *Nacarino*, 668 F. Supp. 3d at 896; *see also Jeong*, 2022 WL 174236, at *27.

Sonner aside, plaintiffs must still plead an actionable wrong. *See Hammerling*, 615 F. Supp. 3d at 1096; *see also Rojas-Lozano v. Google, Inc.*, 159 F. Supp. 3d 1101, 1120 (N.D. Cal. 2016) (“[W]hen a plaintiff fails to sufficiently plead an actionable misrepresentation or omission, his or her restitution claim must be dismissed.”) (cleaned up); *see Swearingen v. Healthy Beverage, LLC*, No. 13-CV-04385-EMC, 2017 WL 1650552, at *5 (N.D. Cal. May 2, 2017) (dismissing unjust enrichment claim because “it depend[ed] on a finding that Plaintiffs’ relied to their detriment on Defendants’ misrepresentations”). Here, as discussed in more length above, plaintiffs

have not plausibly pled that they relied on a misrepresentation or omission when deciding to use the CapCut app. *See supra* at 32–33; *see also Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 933 (N.D. Cal. 2012) (“[A]s plaintiff has failed to sufficiently plead an actionable misrepresentation or omission, his restitution claim must be dismissed.”).

Accordingly, Count XIII is dismissed without prejudice.

L. Biometric Information Privacy Act (Count XIV)

1. “Biometric Identifiers”

Finally, plaintiffs seek relief under Sections 15(b), (c), (d), and (e) of the Illinois Biometric Information Privacy Act (“BIPA”), 740 ILCS 14/15(b)–(e). BIPA forbids the unauthorized collection, storing, and disclosure of “biometric identifiers” and “biometric information.” 740 ILCS 14/15(b), (d); *see also Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1090 (N.D. Ill. 2017) (citing 740 ILCS 14/1 *et seq.*). The statute defines “biometric identifier” as a “retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 Ill. Comp. Stat. 14/10.

Plaintiffs raise two types of alleged “biometric identifiers” in their complaint: scans of facial geometry and voiceprints taken from user videos. According to defendants, plaintiffs’ BIPA claims fall short because plaintiffs lack “specific factual allegations’ demonstrating that the data is or readily could be used by Defendants to identify them.” [38] at 19–20 (quoting *Castelaz v. Estee Lauder Companies., Inc.*, No. 22 CV 5713, 2024 WL 136872, at *1 (N.D. Ill. Jan. 10, 2024)). In their view, they are

not collecting “biometric identifiers” as long as they are not matching (or are capable of matching) the biometric data to a person’s identity.

As with all questions of statutory interpretation, the “best evidence of legislative intent is the language used in the statute itself, which must be given its plain and ordinary meaning.” *Paris v. Feder*, 179 Ill.2d 173, 177 (1997). “Where the statutory language is clear and unambiguous, it will be given effect without resorting to other aids for construction.” *People v. Fitzpatrick*, 158 Ill. 2d 360, 364–65 (1994).

Here, scans of facial geometry and voiceprints are straightforwardly “biometric identifiers” under the text, which defines “biometric identifiers” to include both “voiceprint[s]” and “scan[s] of ... face geometry.” *Id.* Despite defendants’ assertions, the definition itself does not require that defendants *actually* use the data to identify individuals. Various courts in this District have already reached this conclusion. *See, e.g., Konow v. Brink’s, Inc.*, 721 F. Supp. 3d 752, 755 (N.D. Ill. 2024) (“[A] defendant may violate BIPA even without using technology for the purpose of identifying an individual; instead, BIPA bars the collection of biometric data that merely *could* be used to identify a plaintiff.”); *Robinson v. Lake Ventures LLC*, No. 22 CV 6451, 2023 WL 5720873, at *7 (N.D. Ill. Sept. 5, 2023); *Bell v. Petco Animal Supplies Stores, Inc.*, No. 22 C 6455 (N.D. Ill. May 11, 2023), ECF No. 23; *Carpenter v. McDonald’s Corp.*, 580 F. Supp. 3d 512, 518 n.2 (N.D. Ill. 2022).

Defendants cite to a trio of opinions that have dismissed claims that failed to allege that defendants were *capable* of identifying users based on the biometric data they collected. *See Clarke v. Aveda Corp.*, 704 F. Supp. 3d 863, 866 (N.D. Ill. 2023);

Castelaz, 2024 WL 136872, at *7; *Daichendt v. CVS Pharmacy, Inc.*, No. 1:22-cv-3318, 2022 WL 17404488, at *5 (N.D. Ill. Dec. 2, 2022) (“*Daichendt I*”). In these cases, though, the problem was that plaintiffs had not even “allege[d] that they provided defendant with any information, such as their names or physical or email addresses, that could connect the voluntary scans of face geometry with their identities.” *Daichendt*, 2022 WL 17404488, at *5. Indeed, in *Daichendt*, the Court subsequently allowed plaintiffs’ BIPA claim to proceed after they amended their complaint to plausibly allege that defendant collected their “real-world identifying information.” *Daichendt v. CVS Pharmacy, Inc.*, No. 1:22-cv-3318, 2023 WL 3559669, at *1 (N.D. Ill. May 4, 2023) (“*Daichendt II*”). Here, in contrast, plaintiffs have alleged that CapCut “collects a broad array of private and personally identifiable data” that (at least in theory) could have been used to connect plaintiffs’ voiceprints and face scans to their identities. [22] ¶¶ 100, 317. Thus, it is clear from the face of plaintiffs’ complaint that defendants were capable of using the data to identify them, even if they did not actually do so.

Defendants also contend that plaintiffs’ allegations related to the use of voiceprints fail for lack of specificity. *See, e.g.*, [31] at 31 (plaintiffs’ complaint “is devoid of any well-pleaded factual allegations demonstrating that CapCut collects or uses voiceprints”). But plaintiffs plainly allege that CapCut collects plaintiffs’ voiceprints, *see, e.g.*, [22] ¶¶ 303, 314–315, and they support these allegations with further detail that ByteDance, which runs CapCut, has filed patent applications for voiceprint technology and that subsidiaries of ByteDance have spoken publicly about

“speaker identification,” *id.* ¶ 325. Because the Court accepts these allegations as true at the pleading stage, *see Iqbal*, 556 U.S. at 678, plaintiffs plausibly state that the CapCut app collects voiceprints.

Defendants also argue that plaintiffs fall short of alleging CapCut collects “scans of face geometry” through user videos, *see* [38] at 20–21, but the Court disagrees. Plaintiffs allege, for example, that “Defendants employ engineers in fields such as computer vision, convolutional neural network, and machine learning, all of which are used to generate the face geometry scans that Defendants derive from the videos of CapCut users.” [22] ¶ 320. Moreover, courts in this District and elsewhere agree that the data gleaned from analyzing facial geometry within videos can constitute a “biometric identifier” under BIPA. *Deyerler*, 2024 WL 774833, at *4 (defendants used software to record and analyze videos of candidates’ facial geometry during job interviews); *Wilk v. Brainshark, Inc.*, 21 C 4794, 2022 WL 4482842, at *5 (N.D. Ill. Sept. 27, 2022) (defendants used facial-mapping technology to analyze facial features in sales professionals’ videos); *Colombo v. YouTube, LLC*, 679 F. Supp. 3d 940, 944 (N.D. Cal. 2023) (defendants collected and stored facial scans from a YouTube video-editing tool). The Court finds these cases persuasive and likewise concludes that plaintiffs’ allegations regarding voiceprints and face scans are enough under the circumstances.

Defendants offer additional reasons why plaintiffs have not plausibly stated claims under 740 ILCS 14/15(c), (d), and (e), which the Court addresses in the discussion that immediately follows. However, defendants do not offer any additional

reason why plaintiffs’ claim under Section 15(b) should not stand. Therefore, viewing the allegations in the light most favorable to plaintiffs, the Court finds that they have stated a claim for relief under Section 15(b).

2. Defendants’ Remaining BIPA-Related Arguments

a. Section 15(c)

According to Section 15(c) of BIPA, “[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person’s or a customer’s biometric identifier or biometric information.” 740 ILCS 14/15(c). In defendants’ view, plaintiffs have not alleged that defendants “sell, lease, trade, or otherwise profit from” their data. In response, plaintiffs maintain that defendants “trade” their data by giving their videos to TikTok in exchange for TikTok running CapCut advertisements within its application. *See* [36] at 39–40 (citing [22] ¶¶ 68–70).

As a preliminary matter, plaintiffs’ contention that TikTok “trades” advertising in exchange for CapCut’s biometric data does not appear on the face of plaintiffs’ complaint. [22] ¶¶ 68–70. The complaint only alleges that “ByteDance utilized the popular TikTok app to heavily promote its new CapCut video editing app to users in the United States”—not that TikTok ran the ads in exchange for receiving biometric data. *Id.* ¶ 68. More fundamentally, the complaint fails to allege that TikTok ever received “biometric identifiers” from CapCut. At most, it alleges that TikTok received videos to use in advertisements, but photographs and videos are not themselves biometric identifiers. *See Rivera*, 238 F. Supp. 3d at 1096; *Patterson*, 593

F. Supp. 3d at 817 (“The statute [] makes clear that a photograph (and perhaps, by extension, a video) is not itself a biometric identifier.”). As the district court in *Rivera* put it: The “bottom line is that a ‘biometric identifier’ is not the underlying medium itself, or a way of taking measurements, but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person.” *Rivera*, 238 F. Supp. 3d at 1096. Here, plaintiffs have not alleged that defendants ever shared anything but the “underlying medium” (their videos) with TikTok.¹⁰

Plaintiffs also allege that defendants “otherwise profited from” their data in several ways, including the development of artificial intelligence technologies, targeted advertising, and the development of patents. [36] at 39. They further suggest that defendants incorporate plaintiffs’ biometric identifiers as a “necessary element” into their business model. *Id.* at 40 (citing *Flores v. Motorola Sols., Inc.*, 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021)). Like at least two other district courts, the Court is not inclined to adopt such a broad understanding of Section 15(c). *See Delgado v. Meta Platforms, Inc.*, 718 F. Supp. 3d 1146, 1160–61 (N.D. Cal. 2024); *Vance v. Microsoft Corp.*, 534 F. Supp. 3d 1301, 1309 (W.D. Wash. 2021). It is “insufficient to allege, without more, that a company used biometric data to improve its technologies.” *See Delgado*, 718 F. Supp. 3d at 1160–61. *Vance* summarized the concern as follows:

¹⁰ This analysis does not affect the Court’s earlier conclusion that plaintiffs adequately stated the collection of their biometric identifiers under Section 15(b). Plaintiffs allege that defendants *collect* more than their underlying videos. For instance, they allege that defendants also generate “face geometry scans” from the videos of CapCut users, [22] ¶ 320, and “scan[s] of ... face geometry” are explicitly listed under BIPA’s definition of “biometric identifiers.” 740 Ill. Comp. Stat. 14/10.

Taken to its logical end, Plaintiffs’ reading of § 15(c) would prohibit the sale of any product containing biometric technology because any such feature had to be developed or built with biometric data. ... For instance, a company could not sell biometric timekeeping systems—or any product with a biometric feature—because it was presumably developed using biometric data. Similarly, no company could use that biometric timekeeping system because it uses employees’ biometric data to streamline operations and decrease costs. Nothing—not BIPA’s statutory language, its stated intent, or any authority analyzing § 15(c)—supports such a broad reading.

534 F. Supp. 3d at 1308 (internal citation omitted).

So where does that leave the meaning of “otherwise profit”? As *Vance* reasoned, “otherwise profit” should be “interpreted in light of the terms that precede it: sell, lease and trade,” which all “contemplate a transaction in which an item is given or shared in exchange for something of value.” *Id.* at 1306; *see also Circuit City Stores, Inc. v. Adams*, 532 U.S. 105, 114–15 (2001) (according to the *ejusdem generis* tool of statutory construction, general words following specific words “embrace only objects similar in nature to those objects enumerated by the preceding specific words”). Thus, “while ‘profit’ may have a broader ‘ordinary meaning,’” “otherwise profit” encompasses “commercial transactions—such as a sale, lease or trade—during which the biometric data is transferred or shared in return for some benefit.” *Id.* at 1307. Applying that definition, none of plaintiffs’ theories suggests defendants “benefited from” using plaintiffs’ biometric data in a for-profit commercial transaction.

The Court is not swayed by plaintiffs’ citation to *Flores*. There, the defendant used biometric data to develop a database that allowed customers to search for facial matches. 2021 WL 232627, at *3. “[W]ithout the identified biometric data, there would be no product to speak of.” *Vance*, 534 F. Supp. 3d at 1309 (citing *Flores*, 2021

WL 232627, at *3). Here, plaintiffs have not alleged that defendants' video-editing business model relies on the collection of plaintiffs' *biometric* data and not the underlying videos. *See id.* (distinguishing *Flores* because plaintiffs had "not alleged that the biometric data is itself so incorporated into Microsoft's product that by marketing the product, it is commercially disseminating the biometric data").

Accordingly, to the extent Count XIV relies on Section 15(c) of BIPA, the count is dismissed.

b. Section 15(d)

Plaintiffs claim defendants violated Section 15(d) of BIPA, which "prohibits a private entity in possession of biometric data from disclosing or disseminating that data except in certain circumstances, such as obtaining a subject's consent." *Patterson*, 593 F. Supp. 3d at 816 (citing 740 ILCS 14/15(d)). Plaintiffs allege that defendants "disseminated" their biometric data by (1) making the data accessible to the CCP, (2) trading user data with entities within ByteDance, and (3) storing the data on separate servers to use in developing patents and artificial technologies.

As for the first theory, for the same reasons discussed in the SCA context, the Court finds plaintiffs' allegations related to data-sharing with the CCP too speculative to state a plausible claim for relief. *See supra* at 21–23. Plaintiffs' second theory fails for the reason already discussed with regard to their Section 15(c) claim: plaintiffs have not alleged that they "trade" biometric data with ByteDance's subsidiaries like TikTok. *See supra* at 43–44. Plaintiffs allege defendants "disclosed" and "disseminated" plaintiffs' "biometric identifiers," [22] ¶ 310, but they do not

specify with whom defendants shared the information. Such a conclusory allegation does not suffice. And with respect to plaintiffs' third theory, none of the allegations to which plaintiffs point actually state that their personal data, let alone their biometric data, is disseminated to third parties via a server. [36] at 41. Owing to this lack of detail, plaintiffs' complaint falls short.

Accordingly, to the extent Count XIV relies on Section 15(d) of BIPA, the count is dismissed.

c. Section 15(e)

Section 15(e) of BIPA requires entities to “store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity’s industry.” 740 ILCS 14/15(e).

To state a claim under Section 15(e), a plaintiff must, at the very least, allege what the industry standard of care is and how a defendant’s practices fell short of that standard. *See Delgado*, 718 F. Supp. 3 at 1161 (dismissing plaintiff’s Section 15(e) claim because the “complaint provide[d] no allegations regarding how Meta stores biometric data or how its practices fail[ed] to comply with the reasonable standard of care”). Plaintiffs’ complaint contains no allegations describing the industry standard of care. And, other than merely repeating the allegations already used to support their claims under other BIPA provisions (several of which the Court has just rejected), plaintiffs’ complaint does not offer any insight into how defendants’ practices differed from the standard.

Accordingly, to the extent Count XIV relies on Section 15(e) of BIPA, the count is dismissed.

CONCLUSION

The Court grants in part and denies in part defendants' motion to dismiss. [30]. To summarize: Plaintiffs have sufficiently stated violations of their privacy rights under the California Constitution (Count VI); intrusion upon seclusion (Count VII), larceny (Count XI), and conversion (Count XII) under California law; and BIPA (Count XIV), subject to the limitations detailed above. The remaining claims are dismissed without prejudice, except for the Count II VPPA claim, which is dismissed with prejudice.

The Court grants plaintiffs leave to file a second amended complaint on or before 4/2/25 if they can cure the deficiencies with these claims while still complying with their Rule 11 obligations. *See Runnion ex rel. Runnion v. Girl Scouts of Greater Chic. & Nw. Ind.*, 786 F.3d 510, 519–20 (7th Cir. 2015). If plaintiffs elect not to file a second amended complaint by 4/2/25, the dismissal will convert to a dismissal with prejudice.

Assuming a second amendment is filed, the parties are directed to appear for an in-person status hearing on 4/17/25 at 9:30 a.m. to discuss next steps in the case. One week before the status hearing, on 4/10/25, the parties are directed to file a joint status report with a proposed discovery plan and discussing the parties' interest in pursuing settlement.

A handwritten signature in cursive script, reading "Georgia N. Alexakis".

Georgia N. Alexakis
United States District Judge

Date: 3/3/25