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

LORI WILK, individually and on behalf of all others similarly situated, Plaintiff, v. BRAINSHARK, INC. Defendant.	Case No. 1-21-cv-4794 Judge John Robert Blakey

MEMORANDUM OPINION AND ORDER

In this putative class action, Plaintiff Lori Wilk ("Plaintiff") sues Brainshark, Inc. ("Brainshark") for violating sections 15(a) and 15(b) of the Illinois Biometric Information Privacy Act ("BIPA"), 740 Ill. Comp. Stat. 14/1 et seq, by impermissibly collecting or obtaining her biometric data from a video that she uploaded to Brainshark at her employer's request. [1]. Plaintiff sues on behalf of herself and a putative class of other Illinois residents whose biometric data Brainshark collected. *Id.* Brainshark has moved to dismiss Plaintiff's Complaint under Federal Rule of Civil Procedure 12(b)(6). [21]. For the reasons explained below, the Court denies Brainshark's Motion, [21].

I. Legal Standard

To survive a 12(b)(6) motion, a complaint must set out a short and plain statement of the claim that provide the defendant with "fair notice" of the claim "and the grounds upon which it rests," *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). The complaint must also contain

"sufficient factual matter" to state a facially plausible claim to relief and "allow the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting and citing *Twombly*, 550 U.S. at 556, 570). In analyzing a motion to dismiss, a court must also construe the complaint in the light most favorable to the plaintiff, accept all well-pled allegations as true and draw all reasonable inferences in a plaintiff's favor. *See Iqbal*, 556 U.S. at 678; *Bilek v. Fed. Ins. Co.*, 8 F.4th 581, 584 (7th Cir. 2021).

II. Factual Allegations

The Court draw all facts from Plaintiff's Complaint. [1]. Plaintiff resides in Naperville, Illinois, and previously worked for RQI Partners, LLC ("RQI"). *Id.* ¶ 11. Brainshark, a Massachusetts company, provides AI-powered technology that takes sales professionals' videos and applies facial-mapping technology to identify their emotions and other performance indicators. *Id.* ¶¶ 4–6. To do this, the technology scans individuals' facial geometry and analyzes each second of the video for the seller's emotions. *Id.* ¶¶ 6, 8. Brainshark performs this service for over 1,000 companies, including RQI. *Id.* ¶ 3.

While Plaintiff worked for RQI, RQI contracted with Brainshark to use its AI-technology to provide RQI with a better understanding of its employees' sales acumen. *Id.* ¶ 7. Between November 2020 and mid-2021, at RQI's request, Plaintiff recorded videos of her sales presentations and uploaded them to Brainshark. *Id.* ¶ 11. Brainshark then analyzed Plaintiff's facial geometry in the videos using its technology and shared with RQI the analysis results. *Id.* ¶ 8.

Brainshark did not inform Plaintiff that it planned to collect scans of her facial geometry or how it planned to retain and manage such data. *Id.* ¶¶ 13, 27. Brainshark also did not have a publicly available policy detailing its data collection and management, nor did it provide Plaintiff with a copy of any such policy. *Id.* ¶ 44. Brainshark also did not obtain Plaintiff's informed written consent to collect her biometric data from the videos she sent at RQI's request. *Id.* ¶¶ 14, 46.

Plaintiff alleges that Brainshark is a "private entity" under BIPA 740 ILCS 14/10. *Id.* ¶ 42. She contends that the scans of facial geometry (from the uploaded videos) qualify as "biometric identifiers" as defined by BIPA and Brainshark's collection and use of her biometric information violated sections 15(a) and 15(b) of BIPA. *Id.* ¶ 43.

III. Analysis

Brainshark asserts four arguments in favor of dismissal. First, Brainshark argues that Plaintiff's claims fail pursuant to Illinois' Extraterritorial Doctrine. [21] at 6. Second, Brainshark argues that the Complaint does not plausibly allege that Brainshark violated sections 15(a) or (b) of BIPA. *Id.* at 7–8. Third, Brainshark argues that the Complaint fails because it does not allege the requisite state of mind for monetary damages. *Id.* at 9. Fourth, and finally, Brainshark argues that BIPA violates the First Amendment because it constitutes an unconstitutional restraint on commercial speech. *Id.* at 10–13.

A. The Extraterritorial Doctrine Does Not Apply

Brainshark begins by arguing that the Complaint fails under Illinois' Extraterritorial Doctrine because BIPA does not apply to purely out-of-state conduct and the Complaint fails to allege that Brainshark allegedly took any action in Illinois. [21] at 6.

As Brainshark correctly points out, *id.* at 7, under Illinois' Extraterritorial Doctrine, an Illinois statute only applies to extraterritorial conduct if the statute evinces clear intent for it to have an extraterritorial effect. *See Avery v. State Farm Mut Ins. Co.*, 835 N.E.2d 801, 852 (Ill. 2005). As Brainshark also correctly notes, [21] at 7, BIPA does not include language to suggest that the Illinois legislature intended for it to have an extraterritorial effect. *See Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017) (finding BIPA lacked extraterritorial effect); *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017) (same). Thus, BIPA only governs Brainshark's alleged conduct if it occurred in Illinois. *See Avery*, 835 N.E.2d at 852.

Next, conduct only occurs in Illinois if it occurs "primarily and substantially" in Illinois. *Avery*, 835 N.E.2d at 853. The Illinois Supreme Court in *Avery*—which considered a claim brought pursuant to the Illinois Consumer Fraud Act—explained that to determine this, a court must consider the "totality of circumstances" including such factors as: a plaintiff's residency, the location of the harm, where the parties sent and received communications, and where the defendant carried out any policy at issue. *Id.*

Here, Brainshark argues that the Complaint only alleges that Plaintiff resides in Illinois and uploaded the videos in Illinois. According to Brainshark, this cannot suffice to plausibly suggest that Brainshark's conduct occurred primarily or substantially within Illinois. [21] at 7–8. Instead, Brainshark posits that the conduct only occurs "primarily and substantially" in Illinois if the alleged facial scanning occurred within Illinois. *Id.* Because it did not (or at least the Complaint does not allege that it did), Brainshark argues that BIPA does not apply.

Brainshark's argument, however, draws too narrow a box around the conduct at issue. As *Avery* made clear, courts do not apply a bright-line rule for determining whether the alleged conduct occurred in Illinois but rather they consider the "totality of circumstances." 835 N.E.2d at 854. Although Brainshark's act of scanning Plaintiff's facial geometry may constitute an essential aspect of the alleged misconduct (and Plaintiff does not allege where that occurred), *Avery* teaches that the "place of injury or deception is only one of the circumstances that make up a fraudulent transaction and focusing solely on that fact can create questionable results." *Id.* at 853.[1]

[1] Brainshark, citing *Salkauskaite v. Sephora USA, Inc.*, 18-CV-08507, 2020 WL 2796122 (N.D. Ill. May 30, 2020), also argues that the Court should not consider Plaintiff's or any third-party conduct in determining whether the conduct occurred in Illinois. [21] at 7. The *Salkauskaite* Court, in deciding whether a federal court had personal jurisdiction over a defendant, held that the alleged "contacts must come from the activity of the defendant, not the activity of the plaintiff or a third party." 2020 WL 2796122, at *4. Brainshark does not contest this Court's personal jurisdiction over it, however, so *Salkauskaite* proves inapposite; and indeed, *Avery* explicitly refutes Brainshark's theory because the court confirmed that plaintiff's residency and communications from the plaintiff or other parties remain relevant factors for determining whether the conduct occurred in Illinois. Further, multiple courts have considered relevant third-party conduct in applying *Avery*'s totality-of-the-circumstances test. *See Monroy* 2017 WL 4099846, at *5; *Rivera* 238 F. Supp. 3d at 1100.

Here, the Court finds that, at this stage the proceedings, the Complaint's allegations suffice to plausibly suggest the conduct occurred "primarily and substantially" in Illinois. As Plaintiff points out, [30] at 5–7, courts frequently find it premature to dismiss claims at the pleading stage based upon the extraterritorial doctrine given the doctrine's fact-intensive inquiry. *See Rivera*, 238 F. Supp. 3d at 1102 (holding that application of the extraterritoriality doctrine is fact-intensive and better resolved after discovery at the summary judgment phase of litigation); *Morrison v. YTB Intern., Inc.*, 649 F.3d 533, 538 (7th Cir. 2011) (same); *Vance v. Amazon.com Inc.*, 525 F. Supp. 3d 1301, 1308–09 (W.D. Wash. 2021) (same).

So too here. While the Complaint does not allege where Brainshark analyzed Plaintiff's biometric data, it alleges that Brainshark contracted with Illinois entities, including Plaintiff's employer, to provide its services to clients operating within Illinois. In turn, as part of these services, Brainshark required that the Illinois entities' employees, like Plaintiff, submit videos to it. Plaintiff also alleges that Brainshark sent back to her and her employer (both of whom are in Illinois) analyses of its geometric scans, thereby taking specific actions toward Plaintiff directed at Illinois. Particularly given the nature of the internet, the question of when and where Brainshark saved Plaintiff's videos, and where it conducted its facial scans and analysis remain factual questions for development in discovery. Further, Plaintiff alleges that Brainshark engaged in other misconduct when it failed to provide her with its policies, obtain her consent, or explain how it planned to use and store her biometric data. [1] ¶¶ 41–47. As to these allegations, discovery may reveal relevant

facts such as where Brainshark creates its service policies, how often it communicated with Plaintiff or RQI, and where it stored Plaintiff's data after it evaluated it.

Brainshark points to one case, *McGoveran v. Amazon Web Services, Inc.*, 488 F. Supp. 3d 714 (S.D. Ill. 2020), in which a court found a BIPA complaint failed to allege Illinois conduct. [21] at 7. There, the plaintiff alleged that Amazon call centers, supported by "Amazon Connect," used a service called "Pindrop" to collect, store, and use voice scans for identity authentication without a written policy or informed consent. *McGoveran*, 488 F. Supp. 3d at 715–17. The court granted the defendant's motion to dismiss, finding that the defendant did not intentionally target Illinois citizens, so the court lacked personal jurisdiction. *Id.* at 723.

This case is not *McGovern*. First, *McGovern* dealt with personal jurisdiction under F.R.C.P 12(b)(2) not dismissal under 12(b)(6) pursuant to Illinois' extraterritorial doctrine. Second, Brainshark, unlike the *McGovern* defendant, intentionally contracted with Illinois companies to provide the alleged services; knew that it would provide these services to Illinois residents; communicated with Plaintiff, an Illinois resident; and required Plaintiff, an Illinois resident, to upload videos containing her private data for its use. Overall, at this stage, Brainshark has not shown that Plaintiff's claims run afoul of the extraterritoriality doctrine.

B. Plaintiff Plausibly Alleges that Brainshark Collected Her Biometric Information

Next, Brainshark argues that the Complaint does not allege a § 15(b) violation because it only collected videos not biometric information. [21] at 7–8. Plaintiff

disagrees, arguing that Brainshark obtained face geometry scans from these videos and § 15(b) applies to face geometry scans.

Section 15(b) states that:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject…in writing that a biometric identifier and biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier and biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier….

740 ILCS 14/15(b). Next, BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. It also includes a long list of things that do not qualify as biometric identifiers including, as relevant here, "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color." *Id*. Finally, it defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual," but that "biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers." *Id*.

Here, Brainshark insists that it only collected a video of Plaintiff, which does not show it collected her biometric information. It argues that a "video of a face" does not clearly fall within the definition of "biometric identifier" because the definition does not include "videos" nor define "scan of face geometry." [21] at 3. According to

Brainshark, BIPA also expressly excludes from the definition "photographs", which it argues constitutes "a comparable visual media." [34] at 8.

The statute's text does not support Brainshark's interpretation. First, even if videos and photographs constitute "comparable media" as Brainshark argues, BIPA does not exclude all photographs from its definition of biometric identifiers. Instead, it only excludes "photographs" "used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical description such as height, weight, hair color, or eye color." *Id.* Brainshark's use of Plaintiff's video does not fall under this exception. Further, BIPA's reference to "photographs" indicates that, but for the limited exception not applicable here, photographs can constitute "biometric identifiers." Thus, so too can videos.

Second, Brainshark's focus on how it collected Plaintiff's face geometry—*i.e.*, through a video—ignores that BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *See* 740 ILCS 14/10. Thus, under a plain reading of the text, it does not matter how one collects information, but merely whether the information one collects qualifies as a "biometric identifier."

Here, Brainshark's own marketing and resources confirms that its technology scans videos for facial features. [1] ¶¶ 4–8. Thus, the proper question here is whether a facial feature scan qualifies as a "biometric identifier." The Court finds that it does. In fact, BIPA explicitly defines "biometric identifier" to include a "scan of hand and

face geometry." *Id.* Nonetheless, Brainshark insists that what it collected may not qualify because BIPA does not define a "scan of face geometry." [34] at 6. Yet, Brainshark fails to explain how the term "scan of face geometry" is unclear or how what it collected from Plaintiff's videos does not qualify. To the contrary, multiple other cases have found that what Brainshark allegedly collected and captured here by scanning videos qualifies as collecting and capturing biometric identifiers. *See Rivera*, 238 F. Supp. 3d at 1095 (scanning a photograph for facial features is a facial geometry scan); *In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016) (analyzing claims brought against Facebook based on BIPA and finding that "user-uploaded photographs to create a 'unique digital representation of the face'" constitutes a facial geometry scan); *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 WL 4164452, at *1, 5 (Ill. Cir. Ct. Aug. 27, 2021) (finding that a faceprint created by scanning a photograph constitutes a facial geometry scan).

Overall, Plaintiff adequately alleges that Brainshark violated § 15(b) when it did not seek Plaintiff's prior written consent before it captured and analyzed her face from the videos that she uploaded.

C. Plaintiff Plausibly Alleges Brainshark "Possessed" her Biometric Data

Next, Brainshark argues that Plaintiff's claim based on BIPA's § 15(a) fails because Plaintiff only alleges that Brainshark captured or collected her biometric data, not that it possessed it. [21] at 8. Specifically, Brainshark argues that possession requires "dominion or control" over the biometric data, which the Complaint fails to allege. [21] at 8–9. The Court disagrees.

> Section 15(a) states that:
>
> > A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a). True, courts have required evidence of "dominion or control" to show possession for purposes of § 15(a). *See Heard v. Becton, Dickinson & Co.* 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) (finding no possession where a defendant developed the device that stored fingerprint data but could not access or use that data). Here, however, the Complaint plausibly alleges that Brainshark, in fact, exercised dominion and control over Plaintiff's biometric data. Namely, it alleges that Brainshark obtained access to Plaintiff's uploaded video containing her biometric data; used its technology to scan Plaintiff's facial geometry from those videos and analyze those scans; and then developed reports for Plaintiff's employer. [1] ¶¶ 4–8. These allegations more than suffice to infer Brainshark had dominion or control over Plaintiff's biometric data.

D. Plaintiff Need Not Allege Facts Suggesting State of Mind to Sufficiently Plead a BIPA Claims

Brainshark also argues that Plaintiff's BIPA claims fail because monetary damages require evidence of negligent, intentional, or reckless conduct and the Complaint fails to make such allegations. [21] at 9–10. In response, Plaintiff argues that she does not need to allege facts to establish Brainshark's state of mind and,

regardless, she sufficiently alleges facts to plausibly infer that Brainshark acted negligently, intentionally, or recklessly. [30] at 11–13.

Under 740 ILCS 14/20(1)(2), a party may recover damages over $1,000 for negligent violations and over $5,000 for reckless or willful violations. Such damages, however, constitute but two of multiple remedies that a plaintiff may obtain for a BIPA violation. *See BBL, Inc. v. City of Angola*, 809 F.3d 317, 325 (7th Cir. 2015) ("BIPA contains four remedies available to prevailing plaintiffs in BIPA cases"); *Sosa v. Onfido, Inc.*, 20-cv-4247, 2022 WL 1211506, at *9 (N.D. Ill. Apr. 25, 2022) ("liquidated damages are requests for a particular type of remedy should [Plaintiff] prevail on his underlying BIPA claim); *Cothron v. White Castle Sys., Inc.*, 467 F.Supp.3d 604, 615 (N.D. Ill. 2020) (holding that statutory damages, declaratory relief, and injunctive relief are various forms of relief for a single claim).

Here, in addition to monetary damages, Plaintiff also seeks an injunction against Brainshark, reasonable attorneys' fees and costs, and other relief deemed appropriate. [1] ¶ 47. Thus, even if Plaintiff failed to adequately allege a basis for monetary damages for negligent, intentional, or reckless conduct, that does not warrant dismissal of her BIPA claims. *Davis v. Passman*, 442 U.S. 228, 239 (1979) ("a 'cause of action' is analytically distinct" from, and secondary to, the question of "what relief, if any, a litigant may be entitled to receive."). Courts repeatedly hold that a plaintiff need not "show his entitlement to" the "precise forms of relief" that he seeks at the pleading stage. *Sosa*, 2022 WL 1211506, at *10; *Jones v. Butler*, 663 F. App'x 468, 470 (7th Cir. 2016) (holding that a demand for relief is not part of the

claim); *Cothron*, 467 F. Supp. 3d at 615 ("Rule 12(b)(6) does not require [Plaintiff] to plead the facts that will determine the amount of actual damages she may be entitled to recover.").

In arguing to the contrary, [21] at 10, Brainshark relies upon *Rogers v. CSX Intermodal Terminals, Inc.*, which dismissed a BIPA claim because the complaint only included conclusory allegations about the defendant's state of mind, 409 F. Supp. 3d 612, 619 (N.D. Ill. 2019). The court that issued *Rogers*, however, later came to the opposite conclusion in *Sosa v. Onfido*, 20-cv-4247, 2022 WL 1211506 (N.D. Ill. Apr. 25, 2022). In so doing, it explicitly acknowledged and rejected its prior reasoning in *Rogers*, noting that "several decisions that we did not consider in *Rogers* (and many of which did not issue until after *Rogers*) have convinced us that our conclusion today is the correct one." *Sosa*, 2022 WL 1211506, at *10 n.7. In other words, the court that issued *Rogers* agreed that it had gotten it wrong.

IV. BIPA Does Not Violate the First Amendment

Finally, because Brainshark's non-constitutional arguments fail, the Court turns to Brainshark's arguments that BIPA violates the First Amendment because its use of facial geometry scans constitutes commercial speech and BIPA constitutes a content-based restriction of this commercial speech that is subject to, and cannot withstand, strict scrutiny. [21] at 10–14.

In response, Plaintiff argues that BIPA only restricts how one may collect biometric information and the Seventh Circuit has held that restricting the collection or possession of such information does not restrict speech. [30] at 14–16. In the

alternative, Plaintiff also argues that, even if does, BIPA is not a content-based restriction requiring strict scrutiny; rather, at most, it remains subject to intermediate scrutiny, which it withstands. *Id*. at 21.

The First Amendment applies to the states through the Fourteenth Amendment and prohibits them from enacting laws that restrict speech or expression. *See Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015); *Tagami v. City of Chi.*, 875 F.3d 375, 378 (7th Cir. 2017). Thus, as a threshold point, for a law to implicate the First Amendment, it must regulate speech or expressive conduct. *Cornelius v. NAACP Legal Def. & Educ. Fund, Inc.*, 473 U.S. 788, 797, (1985); *see also Doe v. City of Lafayette*, 377 F.3d 757, 764 (7th Cir. 2004) (en banc) (finding First Amendment doctrine inapplicable "because there [was] no expression at issue").

As a preliminary point, in construing constitutional arguments, a court must narrowly analyze the issues, avoiding unnecessary decision-making. *Miller v. Downey*, 915 F.3d at 464; *see also Hegwood v. City of Eau Claire*, 676 F.3d 600, 603 (7th Cir. 2012) (the court should only consider the exclusive facts of this case to avoid an overbroad ruling). While Brainshark argues that BIPA, as a whole, violates the First Amendment, [21] at 10–13, Plaintiff only sues for violation of §§ 15(a) and (b). Thus, the Court only considers the constitutionality of these provisions.

Next, a statute may be attacked as unconstitutional on its face or as applied. *See Hegwood v. City of Eau Claire*, 676 F.3d 600, 603 (7th Cir. 2012). Here, the Court analyzes Brainshark's arguments as an as-applied challenge only, since Defendant argues that these provisions unconstitutionally restrict its commercial speech made

using the biometric information specifically at issue in this case—namely, Plaintiff's facial geometry scans.

The Court begins by examining whether §§ 15(a) or (b) regulates speech. Section 15(a) requires entities that possess biometric data to maintain retention policies and § 15(b) limits how an entity may collect biometric data. 740 ILCS 14/15(a) and (b). Neither provision, however, restricts how an entity may use that biometric data once collected. *Id.* Brainshark insist that restricting access to information still restricts commercial speech, [21] at 10–14, while Plaintiff argues that it does not, [30] at 14–16.

Dahlstrom v. Sun-Times Media, LLC, 777 F.3d 937 (7th Cir. 2015), which Plaintiff cites, controls. In *Dahlstrom*, officers sued the Sun-Times Media, LLC for violating the Drivers' Privacy Protection Act ("DPPA") by obtaining their birth date, height, weight, hair color and eye color from Illinois motor vehicle records. 777 F.3d at 939. Sun-Times moved to dismiss, arguing that the DPPA, which prohibits persons from knowingly obtaining individual-identifying information from motor vehicle records, violated the Sun Times' First Amendment rights to free speech and freedom of the press. *Id.*

The Seventh Circuit disagreed. As relevant here, the court held that the DPPA's "prohibition on obtaining information from driving records" only limited "*access* to information" and, thus, did not restrict speech. *Id*. at 947–49.[2] The Sun

[2] *Dahlstrom* also considered DPPA's restriction on disclosing personal information from driving records. Although § 15(d) of BIPA restricts how a private entity may disclose biometric information, Plaintiff does not sue Brainshark for violating § 15(d). Thus, the Court does not consider the constitutionality of § 15(d) or examine *Dahlstrom*'s analysis of disclosure restrictions.

Times had argued that restricting access to information effectively restricted its speech because it restricted the "ability to gather and report the news." *Id*. at 947. The court found, however, that the First Amendment does not give anyone a constitutional right to information and that, in fact, there exists numerous constitutionally-permissible laws that limit public access to sensitive information. *Id*.

Like *Dahlstrom*, BIPA §§ 15(a) and 15(b) only restrict how a private entity may access someone's biometric information. That is, these provisions merely require that entities who wish to collect biometric data first obtain informed consent to do so, and develop and make known policies relating to data retention. Brainshark complains that Plaintiff's facial geometry is essentially public information because she (assumedly) constantly exposes her face in public and the government cannot restrict its access to public information. But *Dahlstrom*—which also involved many "public" personal characteristics such as height, hair and eye color—held that the First Amendment simply does not give the public the right to access information.

In arguing that BIPA restricts speech, Brainshark does not try to distinguish *Dahlstrom* or even acknowledge it. Instead, Brainshark relies on *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 562 (2011) and *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999). *See* [21] at 10–11. Only *Sorrell* binds this Court but, regardless, both remain distinguishable.

First, *Sorrell* involved a Vermont law that restricted pharmacies' sale, disclosure, and use of data about physicians' prescribing practices for marketing purposes. 564 U.S. at 562. The Court held that the law restricted commercial speech

because, rather than just restrict access to the information, it restricted disclosure and use of that information. *Id*. at 562–64.

Sorrell differs from this case in a key respect. There, the provisions at issue expressly restricted how pharmacies and others may sell, disclose, and use prescriber-identifying information. *Id*. at 558–59. Here, in contrast, §§ 15(a) and (b) do not restrict how Brainshark may use biometric data, it merely restricts how it may obtain it in the first place. The restrictions at issue in *Dahlstrom*—which the Seventh Circuit issued four years after *Sorrell*—remain a much closer analogy to the restrictions here.

Brainshark's second case, *West*, is similarly distinguishable. There, the Tenth Circuit examined a regulation that required telecommunication companies to obtain prior customer consent before using certain customer network information for marketing purposes. 182 F.3d at 1228–29. The court found that the regulation restricted commercial speech because it limited how it could use information it already possessed to target particular audiences. *Id*. Again, the regulation in *West* remains distinguishable from §§ 15(a) and (b) of BIPA because it regulated how the telecommunications could use data that it already lawfully possessed. In contrast, §§ 15(a) and (b) merely restrict how an entity may obtain data in the first place.

Overall, based upon *Dalstrom*, this Court finds that BIPA §§ 15(a) and (b) do not restrict Brainshark's speech and therefore do not implicate the First Amendment. Accordingly, the Court need not analyze whether these provisions pass constitutional muster (either through strict or intermediate scrutiny) and, in fact, it should not

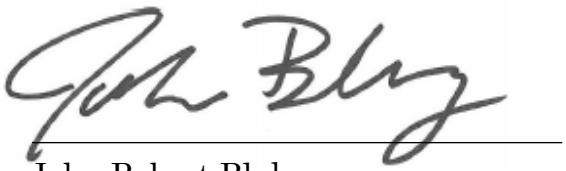
proceed further since a court must avoid making unnecessary constitutional decisions. *Miller v. Downey*, 915 F.3d 460, 464 (7th Cir. 2019) (citing *ISI Int'l, Inc. v. Borden Ladner Gervais LLP*, 256 F.3d 548, 552 (7th Cir. 2001)).

V. Conclusion

For the reasons explained above, the court denies Brainshark's motion to dismiss [21].

Dated: September 27, 2022

Entered:



John Robert Blakey
United States District Judge