2024 WL 4213302
Only the Westlaw citation is currently available.
United States District Court, S.D. Illinois.

Rebecca HARTMAN, Joseph Turner, R.H., a Minor, by and through her Guardian and Next of Friend Rebecca Hartman, and E.T., a Minor, by and through his Guardian and Next of Friend Joseph Turner, on behalf of themselves and all other persons similarly situated known and unknown, Plaintiffs,

v.

META PLATFORMS, INC., Defendant.

Case No. 3:23-CV-02995-NJR
|
Signed September 17, 2024

Attorneys and Law Firms

Ryan A. Keane, Tanner Addison Kirksey, Keane Law LLC, Saint Louis, MO, for Plaintiffs.

Lauren R. Goldman, Lefteri J. Christos, Michael Brandon, Seton Hartnett, Gibson Dunn & Crutcher LLP, New York, NY, Matt Provance, Daniel Thomas Fenske, Mayer Brown LLP, Chicago, IL, for Defendant.

MEMORANDUM AND ORDER

ROSENSTENGEL, Chief Judge:

***1** In this putative class action lawsuit, Plaintiffs allege that Defendant Meta Platforms, Inc. ("Meta" or "Defendant") violated the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), by improperly collecting and possessing biometric identifiers and information through its Facebook Messenger and Messenger Kids applications (collectively "Messenger Applications"). (Doc. 23-2). Plaintiffs' theory is that Meta collects peoples' "face geometries" when they use the Messenger Applications' filters and effects (*e.g.*, bunny ears and flower crowns), and that this practice fails to comply with BIPA's requirements. *Id.* Plaintiffs bring this action on behalf of themselves and other Illinois citizens whose face geometries were allegedly collected between June 28, 2018, and the date of judgment in this case. [1]

BACKGROUND

Meta released Facebook Messenger in August 2011 and Messenger Kids in December 2017. Compl. at ¶ 2 (Doc. 23-2). The Messenger Applications are widely available in popular app stores such as the Google Play App Store and the Apple App Store. *Id.* The named Plaintiffs are long-time users of the Messenger Applications: Rebecca Hartman and Joseph Turner have used Facebook Messenger for "ten-plus years," whereas their minor children, including R.H. and E.T., have used Messenger Kids for "several years." *Id.* at ¶¶ 121, 122.

Until May 2022, the Messenger Applications included facial recognition technology known as "augmented reality" or "AR." *Id.* at ¶¶ 64, 65. AR, as shown below, enabled users to superimpose filters, masks, emojis, and other effects while communicating with their contacts. *Id.* at ¶¶ 66, 76.

***2** This technology allegedly used "scans of face geometry to identify individuals' location[s], expressions, and movements" in real time so that filters and effects could be applied. *Id.* at ¶¶ 73, 74. The resulting facial geometry scans "model[ed] users [sic] faces and track[ed] [their] expressions" based on an "estimation of the location of parts of users' faces." *Id.* at ¶¶ 72, 73. Meta then "collect[ed] the Biometric Data of each child and adult user who utilize[d] an effect or filter," and stored it locally on a user's operating device and on its own servers. *Id.* at ¶¶ 74, 78, & 82.
Meta retains control over the data it collects, regardless of where it is stored. *Id.* at ¶¶ 92, 93. It controls data stored on its servers because it "owns, operates, and controls" them. *Id.* at ¶ 92. This, in turn, gives Meta "exclusive control over the process by which Biometric Data is harvested and stored on its servers." *Id.* In addition, Meta "possesses data stored locally on [Plaintiffs'] devices because it has complete and exclusive control" over it through its operation of the Messenger Applications. *Id.* at ¶ 93.

All of this happened without users' knowledge and consent. *Id.* at ¶ 2. Indeed, Meta allegedly did not inform Illinois users that their biometric data was being collected when they used the AR filters on the Messenger Applications. *Id.* at ¶ 126. Meta also provided no way for users to opt out of its data collection while using the AR filters in the Messenger Applications. *Id.* at ¶ at 89. And considering its collection and possession of biometric data, Plaintiffs allege that Meta failed to publish and follow a compliant data retention and destruction policy under BIPA. *Id.* at ¶¶ 94, 95, 145, & 146; *see also* 740 ILCS 14/15(a).

LEGAL STANDARD

A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) "tests whether the complaint states a claim on which relief may be granted." *Richards v. Mitcheff*, 696 F.3d 635, 637 (7th Cir. 2012). This "generous standard" requires courts to accept the plaintiff's factual allegations as true and draw all inferences in his or her favor. *Domanus v. Locke Lord LLP*, 847 F.3d 469, 479 (7th Cir. 2017); *Reynolds v. CB Sports Bar, Inc.*, 623 F.3d 1143, 1146 (7th Cir. 2010) (quotation marks and citation omitted). To survive a Rule 12(b)(6) motion, the plaintiff only needs to allege enough facts to state a claim for relief that is plausible on its face. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A plaintiff need not plead detailed factual allegations, but must provide "more than labels and conclusions, and a formulaic recitation of the elements." *Id.* at 555. Taken together, the factual allegations contained within a complaint must "raise a right to relief above the speculative level, ... on the assumption that all the allegations in the complaint are true (even if doubtful in fact)." *Id.* (internal citations omitted).

DISCUSSION

A. The BIPA Framework

BIPA regulates the collection, retention, use, and destruction of people's "biometric identifiers" and "biometric information" in Illinois. A "biometric identifier" is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[2] 740 ILCS 14/10. "Biometric information" is defined 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." *Id.*

***3** Private entities that collect and retain biometric identifiers and information must take certain steps to ensure that such information is securely and transparently handled. *See* 740 ILCS 14/15(a)-(b). Under section 15(a), "[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" within a certain amount of time. 740 ILCS 14/15(a). And, perhaps unsurprisingly, the entity must then *comply with* its biometric data retention and destruction policy.[3] *Id.*; *Patterson v. Respondus, Inc.*, 593 F. Supp. 3d 783, 802 (N.D. Ill. 2022).

Section 15(b) prohibits a private entity from "collect[ing], captur[ing], purchas[ing], receiv[ing] through trade, or otherwise obtain[ing] a person's or a customer's biometric identifier or biometric information," unless it first provides certain disclosures and obtains the subject's informed written consent. 740 ILCS 14/15(b). Private entities are also prohibited from selling, leasing, trading, or otherwise profiting from a person's biometric identifier or information. 740 ILCS 14/15(c). They also may not disclose, redisclose, or otherwise disseminate a person's biometric identifier or information, unless they receive the person's consent, the disclosure completes a financial transaction that the person authorized, or the disclosure is required by law. 740 ILCS 14/15(d)(1)-(4).

A person aggrieved by an entity's violation of these requirements may bring an action against the entity under BIPA. 740 ILCS 14/20(a). In such actions, a prevailing plaintiff may recover his or her actual or liquidated damages (whichever is greater), and reasonable attorney's fees and costs. *Id.* §§ (a)(1)-(3); *see also Sosa v. Onfido, Inc.*, 600 F. Supp. 3d 859, 873-74 (N.D. Ill. 2022).

B. Incorporation by Reference

Before reaching the merits of Defendant's arguments, the Court must address a threshold question: which documents are properly considered at this nascent stage of the litigation? This question is before the Court because Meta attached 11 documents to its motion to dismiss which, it contends, "are cognizable," even though several of them are not mentioned in Plaintiffs' complaint. *See* Decl. of Lauren R. Goldman (Doc. 23-1) (listing exhibits to Meta's motion to dismiss and urging Court to consider them). This inquiry requires the Court to evaluate the following documents (attached to Meta's motion to dismiss as Exhibits A through K) to determine whether they may be considered at the pleading stage:

***4** • **Exhibit A:** A copy of Plaintiffs' complaint filed on July 6, 2023. (Doc. 23-2).

- **Exhibit B:** Messenger Kids' Face and Hand Effects Privacy Notice, published in 2023. (Doc. 23-3).
- **Exhibit C:** Facebook Messenger's Face and Hand Effects Privacy Notice, published in 2023. (Doc. 23-4).
- **Exhibit D:** Meta's Terms of Service, last revised July 26, 2022. (Doc. 23-5).
- **Exhibit E:** Messenger Kids' Terms of Service, last revised February 4, 2020. (Doc. 23-6).
- **Exhibit F:** Messenger Kids' Privacy Policy, last revised December 15, 2022. (Doc. 23-7).
- **Exhibit G:** Facebook's Sign-up Webpage, published in 2023. (Doc. 23-8).
- **Exhibit H:** Messenger Kids' Sign-up Webpage, publication date unknown. (Doc. 23-9).
- **Exhibit I:** An article titled "Introducing Messenger Kids, a New App for Families to Connect," by Loren Chang, Meta's Product Management Director, published December 4, 2017. (Doc. 23-10).
- **Exhibit J:** An article titled "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business," published by the Federal Trade Commission, publication date unknown. (Doc. 23-11).
- **Exhibit K:** An article titled "Messenger Kids," published in the Facebook Messenger Help Center in 2023. (Doc. 23-12).

As a general matter, courts may consider only the plaintiff's complaint on a motion to dismiss under Rule 12(b)(6). *Rosenblum v. Travelbyus.com Ltd.*, 299 F.3d 657, 661 (7th Cir. 2002). Indeed, if on a motion to dismiss, "matters outside the pleadings are presented to and not excluded by the court, the motion must be treated as one for summary judgment under Rule 56." FED R. CIV. P. 12(d). And when that happens, "[a]ll parties must be given a reasonable opportunity to present all the material that is pertinent to the motion." *Id.* But there are exceptions to this rule. First, "written instrument[s]" attached to a complaint as exhibits are considered part of the complaint "for all purposes." FED. R. CIV. P. 10(c); *see also Thompson v. Ill. Dep't of Prof. Reg.*, 300 F.3d 750, 753 (7th Cir. 2002) ("The consideration of a [Rule] 12(b)(6) motion is restricted solely to the pleadings, which consist generally of the complaint, any exhibits attached thereto, and supporting briefs."). Second, the "incorporation-by-reference" doctrine allows courts to consider "documents attached to a motion to dismiss if they are referred to in the plaintiff's complaint and are central to his claim." *Brownmark Films, LLC v. Comedy Partners*, 682 F.3d 687, 690 (7th Cir. 2012) (cleaned up). And third, courts may consider "information that is properly subject to judicial notice." *Williamson v. Curran*, 714 F.3d 432, 436 (7th Cir. 2013); *see also Patterson*, 593 F. Supp. 3d at 803-07 (discussing reviewability of extraneous documents on motion to dismiss BIPA claims).

Plaintiffs' complaint does not attach any documents as exhibits. Thus, Meta invokes the second and third exceptions to the general rule to argue that its exhibits warrant consideration. Ultimately, the decision to consider extraneous documents and, if necessary, convert a motion to dismiss into one for summary judgment is within the Court's discretion. *Hecker v. Deere & Co.*, 556 F.3d 575, 583 (7th Cir. 2009), *abrogation on other grounds recognized by Hughes v. Northwestern Univ.*, 63 F.4th 615, 624 (7th Cir. 2023).

1. Exhibit A

***5** Exhibit A is the easiest one. It is a copy of Plaintiffs' complaint and thus *the* critical document to the resolution of Meta's motion to dismiss. No further discussion is required on this point. The Court will, and indeed must, consider Plaintiffs' complaint to resolve Meta's motion.

2. Exhibits D, E, G, and H

Exhibits D, E, G, and H are not mentioned in Plaintiffs' complaint. They are Meta's Terms of Service (Exhibit D), Messenger Kids' Terms of Service (Exhibit E), a copy of the Facebook Sign-up page showing how users create Facebook accounts for themselves (Exhibit G), and a copy of the Messenger Kids Sign-up page showing how parents create Messenger Kids accounts for their children (Exhibit H).

Meta relies on these documents to lay the groundwork for its argument that California law applies to this dispute, and that Plaintiffs' BIPA claims are consequently not viable as a matter of law. Because the Facebook and Messenger Kids' sign-up pages require a user to agree to Meta's and Messenger Kids' terms of service, and the terms of service select California law to govern disputes between Meta and its users, so the argument goes, these documents establish California as the governing law for this case. And Meta contends that these documents are fair game because they are part of its website and Plaintiffs have cited other parts of the website in the complaint, thus opening the door for the full website to be considered.

But, as noted, these documents are neither mentioned in Plaintiffs' complaint, nor do they appear "central" to their claims as required by the incorporation-by-reference doctrine. Exhibits D and E lay out the terms and conditions of a user's relationship with Meta, but neither mentions anything about biometric data. Exhibits G and H (the sign-up pages) provide a link to the terms and conditions (Exhibits D and E) to which a user must consent, and they ask the user for identifying information like their name, birthday, and gender. (Docs. 23-8 & 23-9). But the sign-up pages also do not mention anything about biometric data. Thus, nothing in these documents suggests their centrality to Plaintiffs' claims that Meta improperly collected biometric data in violation of BIPA. *See Patterson*, 593 F. Supp. 3d at 805 ("To be incorporated by reference, the documents themselves—not just their general category or theme—must be central to the complaint and referred to in it."); *Hogan v. Amazon.com, Inc.*, No. 21 C 3169, 2022 WL 952763, at *3 (N.D. Ill. Mar. 30, 2022) (declining to consider defendant's privacy notice and file retention policy because even though they were "linked" in documents that were considered on motion to dismiss, they were not "central" to plaintiffs' BIPA claims).

Patterson and *Hogan* are particularly instructive and thus worthy of further discussion. *Patterson* involved a BIPA action against Respondus, Inc., a provider of a software program that allowed schools to administer online exams using a student's webcam and microphone to record their testing environment. *Patterson*, 593 F. Supp. 3d at 795. The plaintiffs alleged that the program captured their biometric information without their written consent in violation of BIPA. *Id.* at 795-96. The plaintiffs attached two documents to their complaint: Respondus' terms of use and a copy of its webpage containing its privacy policy. *Id.* at 804. Respondus, in turn, filed a motion to dismiss and attached a document titled "Privacy Center Overview" and a webpage titled "Additional Privacy Information." *Id.* Respondus argued that the two documents it introduced were incorporated into the plaintiffs' complaint by reference because the privacy policy (which the plaintiffs did attach) "links to" the Privacy Center Overview, which, in turn, "links to" the Additional Privacy Information page. *Id.* The court rejected this invitation to expand the record, offering the following commentary:

> ***6** Respondus seems to believe that because Plaintiffs' BIPA claims relate broadly to Respondus' written policies, and Plaintiffs attached only some of the relevant policies to their complaints, Respondus has license to supplement the pleadings at its discretion. That is incorrect. To be incorporated by reference, the documents themselves—not just their general category or theme—must be central to the complaint and referred to in it.

Id. at 804-05 (record citations and quotation marks omitted).

In *Hogan*, the plaintiffs sued Amazon.com, Inc. under BIPA, arguing that its Amazon Photos service included "image recognition technology" that improperly collected users' biometric identifiers. *Hogan*, 2022 WL 952763, at *1. Amazon filed a motion to dismiss with seven attachments, which, it claimed, qualified for review under the incorporation-by-reference doctrine. *Id.* at *2. Although the court considered two of these documents because they were "quoted in the Complaint and are central to Plaintiffs' claims," it declined to consider the other five. *Id.* at *3. Among the documents *Hogan* excluded from its review were Amazon's privacy notice and its file retention policy, even though those documents were "linked" in a document that the court *did* consider. *Id.* Neither of these documents, *Hogan* explained, "specifically mentions how Amazon treats biometric information or identifiers, so they are not central to Plaintiffs' claims." *Id. Patterson* and *Hogan* thus took a cautious approach to the defendants' invitations to expand the record on a motion to dismiss.

Meta, for its part, relies on several other cases for the proposition that once a plaintiff cites a website, the Court may consider the full content of that website on a motion to dismiss. For instance, it relies on a footnote from *Gardener v. MeTV*, 681 F. Supp. 3d 864, 867 n.2 (N.D. Ill. 2023), for the proposition that "Plaintiffs referenced [defendant's] website, including specifically their viewing of its video content, in their complaint, such that its contents can be incorporated by reference." Although the footnote cites *Brownmark*'s discussion of the incorporation-by-reference doctrine, it does not address how the website's contents satisfy the doctrine's centrality requirement. Similarly, in *James v. City of Evanston*, No. 20-cv-00551, 2021 WL 4459508, at *7 n.3 (N.D. Ill. Sept. 29, 2021), the court observed in a footnote that "[b]ecause James referenced Evanston's website in his complaint concerning [sic] its contents could be incorporated by reference." *James* also does not explain how the website in question was central to the plaintiff's claim and thus appropriate for consideration. *Patterson* and *Hogan*, on the other hand, addressed an almost identical issue to the one presented here, and they did so in the context of a BIPA action. They thoroughly explained why certain terms and conditions and privacy notices, documents that are thematically similar to Exhibits D, E, G, and H, did not qualify for consideration on a motion to dismiss. *Patterson*, 593 F. Supp. 3d at 806; *Hogan*, 2022 WL 952763, at *3. These cases are thus more aligned with the facts and posture of this case than *Gardner* and *James*, neither of which addressed a BIPA claim. [4] The Court recognizes that "the broader contents of [Meta's] website ... may be relevant at a later stage of this litigation." *Patterson*, 593 F. Supp. 3d at 805. But for now, "allowing [Meta] to cherry pick portions of [its] website to introduce via a motion to dismiss simply because the complaint implicates [the website] would convert an examination of the complaint into full-blown summary judgment analysis." *Facebook, Inc. v. Teachbook.com LLC*, 819 F. Supp. 2d 764, 773 (N.D. Ill. 2011).

***7** Meta also argues that Exhibits D, E, G, and H may be judicially noticed. Although webpages may be judicially noticed as a general matter, the Seventh Circuit has urged courts to do so cautiously. *Daniel v. Cook Cnty.*, 833 F.3d 728, 742 (7th Cir. 2016); *Pickett v. Sheridan Health Care Ctr.*, 664 F.3d 632, 648 (7th Cir. 2011). Indeed, before the Court could even do what Meta asks, Plaintiffs would have to have an opportunity to be heard because "the [i]nternet contains an unlimited supply of information with varying degrees of reliability, permanence, and accessibility." *Id.* Here, it is entirely unclear whether Exhibits D, E, G, and H even accurately present the terms and conditions of Plaintiffs' relationship with Meta over time. Exhibits D and E (Meta and Messenger Kids' respective terms of service) are dated July 26, 2022, and February 4, 2020, respectively. Plaintiffs, for their part, have used Facebook Messenger for "ten-plus years" and Messenger Kids for "several years" prior to filing this lawsuit in July 2023. These recent versions of Facebook and Messenger Kinds' terms and conditions may have been modified over the years, thus triggering questions of whether a valid agreement was ever reached on *these* terms. *See Patterson*, 593 F. Supp. 3d at 805 (declining to consider recent versions of defendant's terms and conditions submitted with motion to dismiss because "corporate websites can change over time, often in ways not made clear from the face of the pages themselves."). Consistent with this sentiment from *Patterson*, the Court finds that it would be inappropriate to take judicial notice of Exhibits D, E, G, and H at this time. *See Karon v. CNU Online Holdings, LLC*, No. 18 C 7360, 2019 WL 3202822, at *2 (N.D. Ill. July 16, 2019) ("The printed portions of [defendant's] website ... are outside the complaint altogether and inappropriate for judicial notice."); *Mussat v. Power Liens, LLC*, No. 13–cv–7853, 2014 WL 3610991, at *3 (N.D. Ill. July 21, 2014) (finding that "[defendant's] website, without more, is not sufficiently reliable for this Court to take judicial notice of its contents as evidence of a prior business relationship with [plaintiff]."); *Felty v. Driver Solutions, LLC*, No. 13 C 2818, 2013 WL 5835712, at *3 (N.D. Ill. Oct. 30, 2013) (similar). The Court thus declines to consider Exhibits D, E, G, and H in resolving Meta's motion to dismiss.

3. Exhibits I, J, and K

Exhibits I, J, and K are cited in the complaint, and thus, according to Meta, suitable for consideration under the incorporation-by-reference doctrine. Exhibit I is a copy of an article titled "Introducing Messenger Kids, a New App for Families to Connect," by Loren Cheng, Meta's Product Management Director. (Doc. 23-10). Exhibit J is a copy of an article titled "Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business," published by the Federal Trade Commission. (Doc. 23-11). And Exhibit K is a copy of an article titled "Messenger Kids," published in the Facebook Messenger Help Center in 2023. (Doc. 23-12).

These articles did little more than set the stage for Plaintiffs' opening narrative. Exhibit I, as its title suggests, introduces Messenger Kids to the public and explains how parents can set up an account for their children. It is cited in three paragraphs of Plaintiffs' 150-paragraph complaint. These three citations provide the date when Messenger Kids was launched (Doc. 23-2 at ¶ 67), explain the four-step process to set up a Messenger Kids account, *Id.* at ¶ 70, and note that Meta advertised its AR filters for Messenger Kids users, *Id.* at ¶ 77. Exhibit J offers regulatory compliance advice to businesses that collect personal information from children under the age of 13 and are thus subject to the Children's Online Privacy Protection Act ("COPPA"). Plaintiffs cited Exhibit J once in their complaint to support their assertion that federal regulators "recognize[ ]" "[t]he heightened sensitivity of minors' personal data." *Id.* at ¶ 61. And Exhibit K offers a how-to guide for parents and their children as to the operation of Messenger Kids, *e.g.*, how to set up an account, add and remove "friends," and report improper behavior. Exhibit K is not even directly cited in Plaintiffs' complaint; it merely appears within the Facebook Messenger Help Center, which is mentioned in the complaint once. *Id.* at ¶ 102. This one reference alleges that the Help Center acts as a document repository that does not make critical privacy notices and disclosures easily accessible to the public. *Id.*

Conspicuously absent from all three of these exhibits is any mention of biometric data. As a result, the Court has little problem concluding that they are not "central" to Plaintiffs' claims. *See Hogan*, 2022 WL 952763, at *3 (documents attached to motion to dismiss did not "specifically mention[ ] how [defendant] treats biometric information or identifiers, so they [were] not central to Plaintiffs' claims."). At best, these documents provide background information about Messenger Kids as a product offering (Exhibits I and K) and the regulatory environment regarding children's online activity (Exhibit J). Certainly, these documents may be *relevant* to the case; but relevance does not equate to centrality under the incorporation-by-reference doctrine. *Patterson*, 593 F. Supp. 3d at 805. Accordingly, the Court will exclude Exhibits I, J, and K from its consideration of Meta's motion to dismiss.

4. Exhibits B, C, and F

***8** Exhibits B, C, and F present a more difficult question. All three of these documents are cited in Plaintiffs' complaint and they appear relevant to a critical issue in the case: whether, and if so, how Meta collected Plaintiffs' biometric identifiers and information.

Exhibits B and C are nearly identical privacy notices concerning the Messenger Applications' face and hand effects. [5] They explain that "[f]ace and hand effects are augmented reality features that react as people in the scene move, speak and express themselves." (Doc. 23-3 at 2). The technology "estimate[s] the location of parts of your child's face (like their eyes, nose or mouth) and points on their face, eyes or hands." *Id.* Critically, these documents state that "[t]his information is not used to identify you [or your child]," and that Meta "do[esn't] store this information on [its] servers or share it with third parties." (Docs. 23-3 at 2 & 23-4 at 2). Exhibits B and C do state, however, that "[t]he information may be stored on your [or your child's] device to make repeat experiences work better." (Docs. 23-3 at 2 & 23-4 at 2).

These disclosures present important evidence in this case because they explain (i) the type of information that is captured; and (ii) how and where it is stored. Thus, Exhibits B and C address the heart of a BIPA action under section 15(b), which prohibits

a private entity from "collect[ing], captur[ing], ... or otherwise obtain[ing] a person's or a customer's biometric identifier or biometric information," unless it first obtains their informed written consent. 740 ILCS 14/15(b). They also appear highly relevant to a claim under section 15(a), which imposes certain requirements on private entities that are "in possession" of biometric identifiers and information. 740 ILCS 14/15(a). Considering the synergy between the information provided in Exhibits B and C and the legal requirements of the asserted BIPA claims, the Court finds that they are "central" to Plaintiffs' claims and thus eligible for consideration under the incorporation-by-reference doctrine.

But eligibility under the incorporation-by-reference doctrine does not *mandate* the Court's consideration of extraneous documents at the motion to dismiss stage. *See Fin. Fiduciaries, LLC v. Gannett Co.*, 46 F.4th 654, 663 (7th Cir. 2022) (on a motion to dismiss, district court "may" consider documents that satisfy incorporation-by-reference doctrine). And here, consideration of Exhibits B and C would be inappropriate.

The privacy notices at issue were allegedly first "created and published" in 2022. *See* Compl. at ¶ 96, (Doc. 23-2). The publication date of Exhibits B and C as attached to Meta's motion even suggests their publication in the year 2023. [6] The recency of these documents presents two problems for Meta. First, Plaintiffs alleged that that Messenger Applications only utilized AR facial recognition technology until May 2022, the same year or even the year before Exhibits B and C were published. *Id.* at ¶ 64. Thus, Exhibits B and C offer little if any value to Plaintiffs' central allegation that Meta misused its AR technology to violate BIPA *until May 2022*. Second, Exhibits B and C do not allow for an informed review of the terms of Plaintiffs' relationships with Meta over the "ten-plus years" or "several years" that they used the Messenger Applications. Instead, they offer a recent snapshot of Meta's privacy notices and do not account for modifications that may (or may not) have been added over time. This targeted view of the evidence as it existed in 2023 would allow Meta to "amend its opponent's pleading using documents that [Meta] itself could have modified," while Plaintiffs used the Messenger Applications. *Patterson*, 593 F. Supp. 3d at 805. For instance, it is entirely possible that prior versions of the privacy notices contained different language about Meta's collection of biometric data, or that they contained no such language at all. To consider Exhibits B and C at this stage of the case would effectively freeze the evidence in place as it existed in 2023. And for reasons that should be apparent, the Court will not engage in such targeted fact-finding on a motion to dismiss. The court in *Patterson* encountered a similar issue and offered the following commentary:

> ***9** Because Plaintiffs' BIPA claims cover several years, this case may involve factual questions about what [defendant's] policies looked like at different moments in time. There is no basis for preempting that fact-intensive inquiry by concluding, as a matter of law, that these specific versions of [defendant's] webpages govern Plaintiffs' claims.

Id. So too here—to avoid preempting highly factual inquiries into topics like (i) the scope of the Messenger Applications' collection of biometric data (if they collected such data at all); (ii) whether, and if so, how, Meta informed Plaintiffs of its collection of biometric data; (iii) where and how such data was stored; and (iv) how these practices may have changed over time, the Court declines to consider Exhibits B and C in resolving Meta's motion to dismiss.

This brings us to the last document Meta asks the Court to consider: Exhibit F. Exhibit F is Messenger Kids' Privacy Notice, which explains the "kinds of information" Meta collects from users, what it does with this information, how parents can control and delete information about their child, and when and how a user's information is shared with law enforcement. (Doc. 23-7). This document presents the same problems as Exhibits B and C: it was last revised on December 15, 2022, less than seven months before Plaintiffs filed this lawsuit, and seven months *after* Meta allegedly stopped offering its AR technology on the Messenger Applications. Thus, it does not capture the full spectrum of terms, conditions, and disclosures that Plaintiffs agreed to while using Messenger Kids. And because the terms that Plaintiffs agreed to and the scope of disclosures regarding biometric data over time are critical to Plaintiffs' BIPA action, the Court declines to consider Exhibit F at this stage as well. *Patterson*, 593 F. Supp. 3d at 805.

Thus, in conclusion, the Court will consider Exhibit A of Meta's motion to dismiss Plaintiffs' complaint (Doc. 23-2). It will not consider Exhibits B through K (Docs. 23-3 through 23-12).

C. Choice of Law

Having resolved one preliminary issue, the Court turns its attention to another: which state's substantive law governs this dispute? Meta contends that California law applies, and that Plaintiffs are consequently barred from bringing claims under BIPA, an Illinois statute. The problem with this argument is that it relies on choice-of-law provisions in Facebook Messenger and Messenger Kids' Terms of Service (Exhibits D and E), which the Court has excluded from its review at this stage of the case. Thus, there is no basis in the record to support the application of California law. So, the Court will consider the viability of Plaintiffs' BIPA claims under Illinois law as that is the legal framework the complaint invokes. *See Patterson*, 593 F. Supp. 3d at 807 (rejecting defendant's choice of law argument on motion to dismiss because it was based on documents the court declined to consider).

To be clear, the Court's decision to apply Illinois law for the limited purpose of testing the legal sufficiency of Plaintiffs' claims does not resolve the question of which state's law ultimately governs this case. Plaintiffs assert that Meta's choice-of-law theory is beset by "factual disputes," and the Court acknowledges this possibility. (Doc. 29 at 7). Indeed, the Court has already explained how the recency of the documents Meta submitted may not capture the evolution of the terms and conditions that governed Plaintiffs' relationship with Meta over time. Discovery may also reveal facts concerning the enforceability of the choice-of-law provisions that Meta seeks to apply. For now, it is enough to recognize that a choice-of-law determination is not possible based solely on Plaintiffs' complaint because the complaint says nothing about it. *See Foisie v. Worcester Polytech. Inst.*, 967 F.3d 27, 42 (1st Cir. 2020) (district courts should refrain from deciding choice-of-law issues when the record is "tenebrous, and the complaint itself leaves unanswered questions about critical aspects of the pertinent facts.").

***10** For these reasons, the Court will defer consideration of the choice-of-law issue pending at least some discovery and further briefing under Rule 56 of the Federal Rules of Civil Procedure. [7]

D. Plaintiffs' BIPA Claims

Meta contests the viability of Plaintiffs' BIPA claims on two grounds. First, it argues that the information at issue is not "biometric" because it is incapable of identifying individual users and people. Second, it contends that Plaintiffs fail to allege that Meta "collected" and "possessed" the information at issue under sections 15(b) and 15(a) respectively.

1. Is the Data at Issue "Biometric"?

Meta argues that the facial scans it allegedly generated are not covered under BIPA because they are not unique to individual users and thus incapable of identifying them. Plaintiffs respond that the ability to identify individual users is irrelevant when, as here, the information at issue is a "biometric identifier" in the form of a "scan of ... face geometry." *See* 740 ILCS 14/10. Plaintiffs' theory is based on a textual comparison of BIPA's definitions of "biometric identifier" and "biometric information." Whereas "biometric information" must be "used to identify an individual," the term "biometric identifier" contains no such requirement. *Id.*

Meta's position, on the other hand, finds support in BIPA's legislative findings and in numerous cases that have addressed the issue. In 2008, the Illinois legislature found that "[b]iometrics ... are biologically unique to the individual," and thus capable of identifying the person to whom they belong. 740 ILCS 14/5(c). It thus appears reasonable to construe the term "biometric identifier" to mean "a biology-based set of measurements ("biometric") that can be used to identify a person ("identifier")," as the Northern District of Illinois did in *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017), and as Meta urges

here. Several courts, including this one, have adopted this construction of the term "biometric identifier" and found that it must be *capable* of identifying an individual. *See e.g.*, *Zellmer v. Meta Platforms, Inc.*, 104 F.4th 1117, 1124 (9th Cir. 2024); *G.T. v. Samsung Elec. Am. Inc.*, —— F. Supp. 3d ——, ——, 2024 WL 3520026, at *7 (N.D. Ill. 2024); *Sosa v. Onfido, Inc.*, 600 F. Supp. 3d 859, 873 (N.D. Ill. 2022); *Hazlitt v. Apple Inc.*, 500 F. Supp. 3d 738, 749 (S.D. Ill. 2020), *vacated on other grounds by In re Apple Inc.*, No. 20-8033, 2021 WL 2451296, at *1 (7th Cir. Jan. 22, 2021); *Martell v. X Corp.*, No. 23 C 5449, 2024 WL 3011353, at *3 (N.D. Ill. June 13, 2024); *Daichendt v. CVS Pharm., Inc.*, No. 22 CV 3318, 2022 WL 17404488, at *5 (N.D. Ill. Dec. 2, 2022). For now, it is not necessary to wade further into this issue because Plaintiffs have imperfectly but sufficiently alleged that the information at issue is capable of identifying them.

***11** Affording the complaint the generous interpretation to which it is entitled, the Court finds that it sufficiently alleges that Meta scanned users' face geometries and that these scans are capable of identifying the people from whom they were taken. Plaintiffs allege that the Messenger Applications relied on AR technology to create "scans of face geometry to identify individuals' location[s], expressions, and movements" in real time. The resulting facial geometry scans "model[ed] users [sic] faces" based on an "estimation of the location of parts of [their] faces." These allegations permit an inference of personalization that supports the uniqueness of each scan based on the user from whom it was taken.

Indeed, the point of this process is to allow users to superimpose filters and effects like bunny ears or cat whiskers on their face. To do so effectively, the bunny ears or cat whiskers would have to appear in a location that creates a plausible appearance. If the filters and effects were applied based on a generic face template that included an oval shape to convey a facial structure, and general outlines of ears, nose, and mouth, the filters and effects could, and often would, create an odd appearance. Bunny ears could appear on the user's forehead or be superimposed in a location that is not connected to the face at all. The technology would have little entertainment or commercial value if it applied these effects in such a non-personalized manner. *See Sosa*, 600 F. Supp. 3d at 871 (extraction of "unique numerical representation of the shape or geometry of each facial image" plausibly constituted scan of face geometry under BIPA); *In re Facebook*, 185 F. Supp. 3d at 1171 (same for "unique digital representation" of users' faces "based on geometric relationship of their facial features").

Meta contends that an "estimation" of the "location" of parts of a person's face cannot possibly identify them. This contention may well be validated in discovery. But to adopt it now requires a factual determination that is not warranted under a faithful application of Rule 12(b)(6). Scanning a person's face to identify the locations of its constituent parts, including eyes, nose, mouth, and ears, creates a geometric representation that is unique to that person. *See Rivera*, 238 F. Supp. 3d at 1091 (scanning for "unique contours" of users' faces and identifying "distinct facial measurements" constituted "biometric identifier"); *ACLU v. Clearview AI, Inc.*, No. 20 CH 4353, 2021 WL 4164452, at *1, *5 (Ill. Cir. Ct. Aug. 27, 2021) (scanning photograph for "data such as the shape of the cheekbones and the distance between eyes, nose, and ears," constituted scan of face geometry). Thus, an "estimation of the location of parts of users' faces" based on a scan of their face is intrinsically unique and could plausibly be used to identify them.

Meta also offers a second argument in support of its contention that the information at issue is incapable of identifying individual users and people, and thus not covered as "biometric" data under BIPA. On this point, Meta claims that Plaintiffs did not provide identifying information that would allow it to match the alleged facial geometry scans to individual users. Without such information, Meta argues, it is impossible to identify people whose face geometry was scanned, regardless of the uniqueness of the data. Meta cites the Northern District of Illinois' decision in *Daichendt v. CVS Pharmacy, Inc.* for the proposition that scans of face geometry, without more, are incapable of identifying individual users, and thus not covered by BIPA. *Daichendt*, 2022 WL 17404488, at *5. But *Daichendt* does not offer Meta the support it claims. In *Daichendt*, the court observed that the plaintiffs failed to allege 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." *Id.* Thus, the court concluded that the plaintiffs "failed to plead the most foundational aspect of a BIPA claim." *Id.*

***12** The allegations here are slightly more robust. Plaintiffs Rebecca Hartman and Joseph Turner, at a minimum, allege that they created usernames and passwords for themselves to set up their Facebook accounts. *See* Compl. at ¶ 70 (Doc. 23-2). They

also allege that Messenger Kids requires a child's name to set up an account for them. *Id.* Although more information would have been helpful, Plaintiffs have sufficiently alleged that they supplied identifying information that Meta could match to their face geometry scans to identify them. These allegations meet the minimum plausibility threshold under Rule 12(b)(6), and thus distinguish this case from *Daichendt*, where the plaintiffs did not provide "any information" that could be matched to their face geometry to reveal their identities. *Daichendt*, 2022 WL 17404488, at *5.

So, crediting the truth of Plaintiffs' allegations and drawing all reasonable inferences in their favor, the Court rejects Meta's argument that the information at issue is incapable of identifying individual users and people, and thus not covered under BIPA.

2. Did the Messenger Applications "Collect" and "Possess" Plaintiffs' Biometric Data?

Count I of Plaintiffs' complaint asserts a claim under 740 ILCS 14/15(b), which prohibits private entities from "collect[ing]" or otherwise obtaining a person's biometric data without their informed written consent. Count II advances a claim under 740 ILCS 14/15(a), which imposes certain requirements on private entities "in possession" of peoples' biometric data. Meta contends that Plaintiffs have failed to state a claim under either section because the complaint lacks the necessary factual allegations to suggest that Meta "collect[ed]" or was "in possession" of biometric data.

BIPA does not define the terms "collect" and "possess." When statutory terms are undefined, the Illinois Supreme Court "assume[s] the legislature intended for [them] to have [their] popularly understood meaning." *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019). Moreover, "if a term has a settled legal meaning, the courts will normally infer that the legislature intended to incorporate that established meaning into the law." *Id.* Fortunately with respect to the terms "collect" and "possess," the Illinois Supreme Court has offered guidance as to their respective meanings. To "collect" means to "to receive, gather, or exact from a number of persons or other sources." *Cothron v. White Castle Sys., Inc.*, 216 N.E.3d 918, 924 (Ill. 2023) (quotation marks and citation omitted). To "possess" means that a person "has or takes control of the subject property or holds the property at his or her disposal." *People v. Ward*, 830 N.E.2d 556, 560 (Ill. 2005).

According to Meta, Plaintiffs "acknowledge" that the only place where the information at issue is stored is on users' personal devices, not on servers or in databases that Meta controls. (Doc. 23 at 27). Thus, so the argument goes, if the information at issue never leaves a user's personal device, there is no way Meta could have "collected" or "possessed" it. And with this concession, Meta argues that Counts I and II are fatally defective. [8]

***13** But the complaint reveals no such concession. In fact, it reveals the opposite. Plaintiffs allege that Meta "collect[ed] the Biometric Data of each child and adult user who utilize[d] an effect or filter," and stored it locally on users' devices *and* on its "servers." Compl. at ¶¶ 74, 78, & 82 (Doc. 23-2). And specifically with respect to biometric data on Meta's servers, Meta retains "exclusive control over the process by which Biometric Data is harvested and stored." *Id.* at ¶ 92. These allegations refute Meta's claim of an "acknowledge[ment]" from Plaintiffs that the information at issue is only stored on users' personal devices.

The allegation that Meta stores Plaintiffs' biometric data on its servers (which the Court accepts as true) also undercuts Meta's legal argument that it did not "collect" or "possess" it. Meta relies on the Illinois Appellate Court's decision in *Barnett v. Apple Inc.* to support its contention that biometric data storage on a user's personal device and nowhere else is fatal to a claim that it "collect[ed]" and "possess[ed]" such data. 225 N.E.3d 602, 611 (Ill. App. Ct. 2022). In *Barnett*, the plaintiffs alleged that their fingerprints and face geometries were stored on their own devices, which the defendant, Apple Inc., had manufactured. *Id.* at 603-04. This information allowed them to unlock their devices and make purchases using their biometric data. *Id.* at 604. But the plaintiffs offered "*no allegation* that Apple stores this information on a separate server or that Apple has ever once prevented a user from deleting her own information." *Id.* at 610 (emphasis added). This factual gap compelled the conclusions that Apple (i) did not "possess" the plaintiffs' biometric data because it never exercised control over it, and (ii) never "collected" it because it "remained in a multitude of different and distinct places, namely the millions of devices of Apple's numerous users." *Id.* at 610, 611.

Barnett is easily distinguishable for the simple reason that Plaintiffs *do* allege that Meta stores their biometric data on its servers as well as on users' personal devices. And because the Court is bound to credit the truth of this allegation over Meta's contention that "the data is stored not on Meta's servers, but rather only on the individual personal devices ... that users themselves control," it must also reject Meta's argument that it could not have "collected" or "possessed" Plaintiffs' biometric data. (Doc. 23 at 27). By scanning peoples' face geometries when they use the Messenger Applications' filters and effects and centrally storing such data on its servers, Meta plausibly "gather[s], or exact[s] [biometric data] from a number of persons or other sources" (collection) and "takes control" of it (possession). *See Heard v. Becton, Dickinson & Co.*, 524 F. Supp. 3d 831, 841 (N.D. Ill. 2021); *Mayhew v. Candid Color Sys., Inc.*, No. 23-cv-2964-DWD, 2024 WL 3650095, at *13 (S.D. Ill. Aug. 5, 2024).

With that, the Court rejects Meta's argument that Plaintiffs' complaint fails to allege that it "collected" or "possessed" their biometric data.

E. COPPA Preemption

Meta's final argument is that the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-06, expressly preempts Plaintiffs' BIPA claims with respect to Messenger Kids. "Under COPPA and its regulations, companies that operate websites and online services marketed toward children must provide certain disclosures about their data collection activities and must safeguard the confidentiality, security, and integrity of the children's personal online information." *Jones v. Google LLC*, 73 F.4th 636, 641 (9th Cir. 2023). The Federal Trade Commission ("FTC") has rule-making authority under COPPA, and it shares enforcement authority with state attorneys general. 15 U.S.C. §§ 6502(b), 6504. Unlike BIPA, however, COPPA does not authorize a private right of action. *Jones*, 73 F.4th at 641.

***14** COPPA's regulatory focus is the online collection of "personal information" from children. 15 U.S.C. § 6502(a)(1). "Personal information" is defined as "individually identifiable information about an individual collected online," including one's name, physical and email addresses, telephone number, social security number, and "information concerning the child or the parents of that child that the website collects online from the child and combines with [one of the aforementioned identifiers]." 15 U.S.C. § 6501(8). Under the FTC's regulations, "personal information" also includes (i) a "persistent identifier," like an internet protocol ("IP") address or device serial number, which "can be used to recognize a user over time and across different Web sites"; (ii) a "photograph, video, or audio file ... contain[ing] a child's image or voice"; and (iii) geolocation information. 16 C.F.R. § 312.2. Operators of websites and online services directed to children are prohibited from collecting their personal information unless they meet certain requirements concerning notice, safekeeping, and transparent handling of such information. 15 U.S.C. § 6502(b). They also must obtain "verifiable parental consent for the collection, use, or disclosure of personal information from children." *Id.* § 6502(b)(1)(A)(ii).

To help accomplish these goals at the federal level, COPPA contains the following express preemption clause:

> No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.

15 U.S.C. § 6502(d). The question is whether this provision preempts Plaintiffs' BIPA claims with respect to Messenger Kids.

The Court begins by recognizing the paucity of authority discussing COPPA's preemptive effect on BIPA actions like this one. Indeed, the parties and this Court have identified only one case that addresses this issue. *See H.K. through Farwell v. Google LLC*, 595 F. Supp. 3d 702, 709-11 (C.D. Ill. 2022). Nevertheless, the Seventh Circuit has provided the analytical framework for an informed preemption assessment in this case.

There are three forms of federal preemption: express preemption, conflict preemption, and field preemption. [9] *Aux Sable Liquid Prods. v. Murphy*, 526 F.3d 1028, 1033 (7th Cir. 2008). "Express preemption applies when Congress *clearly declares* its intention to preempt state law." *Nelson v. Great Lakes Ed. Loan Srvs., Inc.*, 928 F.3d 639, 651-52 (7th Cir. 2019) (emphasis added). Thus, "when the text of a preemption clause is susceptible of more than one plausible reading, courts ordinarily accept the reading that disfavors preemption." *Altria Group, Inc. v. Good*, 555 U.S. 70, 77 (2008) (internal quotation marks omitted). "Conflict preemption applies when there is an actual conflict between state and federal law such that it is impossible for a person to obey both, or when state law stands as an obstacle to fully accomplishing the objectives of Congress." *Nelson*, 928 F.3d at 646-47. Field preemption exists "when federal law so thoroughly occupies a legislative field as to make it reasonable to infer that Congress left no room for the states to act." *Aux Sable*, 526 F.3d at 1033 (citation and internal quotation marks omitted). Regardless of the preemption doctrine under consideration, preemption may not be "lightly applied" because of its potential encroachment on a state's police powers. *Patriotic Veterans, Inc. v. Indiana*, 736 F.3d 1041, 1046, 1049 (7th Cir. 2013). That is why courts consider preemption questions "through a lens that presumes that the state law has not been preempted." *Id.* at 1046.

***15** In *Patriotic Veterans v. Indiana*, the Seventh Circuit confronted the issue of whether the federal Telephone Consumer Protection Act ("TCPA") preempted an Indiana law regulating telemarketing and robocalling. *Id.* at 1044-46. The Indiana law barred the use of "automatic dialing-announcing device[s]" without the recipient's consent. *Id.* at 1044. The TCPA, for its part, prohibited the use of an "artificial or prerecorded voice to deliver a message" without the recipient's written consent, unless the call is "not made for a commercial purpose." *Id.* at 1045. The TCPA also contained a preemption clause in the form of a "savings clause," which stated that it did *not* "preempt any State law that imposes more restrictive intrastate requirements or regulations on" robocalling, or "which prohibits" its use and the use of autodialing technology. *Id.* at 1046. The district court held that any law that was not expressly saved by the savings clause was preempted—*i.e.*, only general *prohibitions* and *intrastate* regulations and restrictions on auto-dialing technology were not preempted. *Id.* Thus, the district court found that the Indiana law was preempted because it was a non-covered regulation under the savings clause. *Id.* at 1047. The Seventh Circuit reversed because this interpretation of the TCPA's savings clause turned the preemption analysis on its head. *Id.* at 1047-48. According to the Seventh Circuit, the district court erroneously "presum[ed] that laws that were not explicitly saved were preempted." *Id.* at 1048. Rather, because "the TCPA says nothing about preempting laws that regulate the interstate use of automatic dialing systems," the court had to "conclude that they are not preempted." *Id.* The takeaway from *Patriotic Veterans* is that courts should avoid expansive interpretations of preemption language in a federal statute when a narrower construction is reasonably available.

Six years later, in *Nelson v. Great Lakes Ed. Loan Srvs.*, the Seventh Circuit considered the preemptive effect of the federal Higher Education Act ("HEA"), which provided that federal student loans "shall not be subject to any disclosure requirements of any State law." 928 F.3d at 642. In that case, the plaintiff alleged that her student loan servicer had made affirmative misrepresentations in its loan-related communications with her and that she relied on these misrepresentations to her detriment. *Id.* The Seventh Circuit reversed the district court's holding that the HEA preempted the plaintiff's claims because the preemption clause was limited to "disclosure requirements," not affirmative misrepresentations that could trigger liability under state law. *Id.* at 649. State consumer protection and tort laws, the court reasoned, "could impose liability on these affirmative misrepresentations without imposing additional disclosure requirements on [the defendant]." *Id.* Accordingly, the plaintiff's claims based on affirmative misrepresentations were not preempted because they did not implicate additional "disclosure requirements." *Id.*

More recently, in *C.Y. Wholesale, Inc. v. Holcomb*, the Seventh Circuit considered the preemptive effect of a federal hemp statute on state criminal laws targeting smokable hemp. 965 F.3d 541, 544 (7th Cir. 2020). In that case, the federal Farm Law of 2018 relaxed restrictions on certain hemp products. *Id.* At the same time, the Farm Law expressly did *not* "preempt[ ] or limit[ ] any law of a State ... that regulates the production of hemp and is more stringent than this subchapter." *Id.* (quoting 7 U.S.C. § 1639p). However, states were barred from "prohibiting the transportation or shipment of hemp or hemp products through the State." *C.Y. Wholesale*, 965 F.3d at 544 (cleaned up). In 2019, Indiana passed a law criminalizing the manufacture, delivery, and possession of "smokable hemp." *Id.* The district court held that the Farm Law expressly preempted the Indiana statute's prohibition on the manufacture, delivery, possession, and financing of smokable hemp. *Id.* at 546. The Seventh Circuit found

this interpretation too broad. *Id.* at 547. The Indiana statute covered "much more than transportation, including the manufacture, financing, delivery, or possession of smokable hemp." *Id.* at 545. And by finding the Indiana law preempted, the district court enjoined the enforcement of parts of it (manufacture, delivery, possession, and financing) that had nothing to do with the target of the preemption clause (transportation). *Id.* at 547. Thus, as in *Patriotic Veterans* and *Nelson*, the court construed the preemption clause narrowly to avoid an unnecessary conflict with state law.

With this decisional authority and the presumption against preemption in mind, the Court returns to COPPA's express premotion clause, which prohibits states from "impos[ing] any liability for commercial activities ... that is inconsistent with the treatment of those activities or actions under this section." 15 U.S.C. § 6502(d). Although *a* preemptive intent is evident here, the statute does not explain what it means for a state law to be "inconsistent" with its "treatment" of covered activities. So, the question is whether BIPA imposes requirements that are "inconsistent" with COPPA's regulation of children's online activity.

***16** Again, the only court to address this question appears to be the Central District of Illinois in *H.K. through Farwell v. Google*, 595 F. Supp. 3d at 709-11. The plaintiffs in that case brought claims under BIPA alleging that Google collected "acoustic details and characteristics of [children's] voices," as well as scans and images of their face geometries. *Id.* at 705. The court emphasized the parties' agreement that Google's alleged conduct also violated COPPA and found that "to allow Plaintiffs to assert H.K.'s claim against Defendant would be "inconsistent with COPPA's treatment" of online data collection from children under 13 because COPPA provides for no private right of action ... whereas BIPA does so explicitly." *Id.* at 710 (internal brackets and citation omitted). The court relied on COPPA's broad definition of "personal information" to find that BIPA's regulation of biometric data "falls squarely in COPPA's orbit," even though "COPPA does not expressly reference biometric data in its statutory text." *Id.* at 711. Thus, the Court held that COPPA preempted Plaintiffs' BIPA claims under sections 15(a) and 15(b). *Id.*

Other courts also have addressed COPPA's preemptive effect, albeit with respect to state laws other than BIPA. In *Jones v. Google*, the Ninth Circuit considered whether COPPA preempted consumer protection and tort claims arising under California, Colorado, Indiana, Massachusetts, New Jersey, and Tennessee law. 73 F.4th at 640. The plaintiffs alleged that Google sent them targeted ads and that this process depended on the collection of "persistent identifiers," like IP addresses, which are covered under COPPA as "personal information." 16 C.F.R. § 312.2. The plaintiffs further alleged that Google collected their persistent identifiers without their consent. *Jones*, 73 F.4th at 640. And like in *H.K.*, the parties agreed that "all of the claims allege conduct that would violate COPPA's requirement that child-directed online services give notice and obtain "verifiable parental consent" before collecting persistent identifiers." *Id.* The district court found that Plaintiffs' claims were expressly preempted because their "core allegations" were "squarely covered" by COPPA. *Id.* at 640-41. The Ninth Circuit reversed. Bearing in mind COPPA's limited preemption of "inconsistent" state laws, the court interpreted that statutory term "to refer to contradictory state law requirements, or to requirements that stand as obstacles to federal objectives." *Id.* at 642. And "state laws that supplement or require the same thing as federal law, do not stand as an obstacle to Congress's objectives and so are not "inconsistent." " *Id.* (cleaned up). So, to preempt state laws that inconsistently "treat[ ]" children's online activity, the court reasoned, did not "evince[ ] clear congressional intent to create an *exclusive* remedial scheme for enforcement of COPPA requirements." *Id.* at 643 (emphasis in original). In short, the absence of a conflict between the plaintiffs' claims and COPPA meant that they were not preempted, even if those causes of action "are parallel to, or proscribe the same conduct forbidden by, COPPA." *Id.* at 644; *accord In re Nickelodeon Cons. Priv. Litig*, 827 F.3d 262, 291-93 (3d Cir. 2016) (intrusion claim under state law not preempted by COPPA).

The Court finds that *Jones* is more aligned with the Seventh Circuit's governing framework to narrowly construe preemption provisions when possible. This conclusion is particularly appropriate where, as here, a harmonious construction of BIPA and COPPA is possible based on their distinct regulatory objectives. *C.Y. Wholesale*, 965 F.3d at 547; *Nelson*, 928 F.3d at 649.

BIPA's subject matter is almost entirely distinct from that of COPPA. BIPA, as noted, regulates "biometric identifiers" and "biometric information." A biometric identifier is "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. "Biometric information" is "any information ... based on an individual's biometric identifier used to identify an individual." *Id.* These biology-based characteristics (biometric identifiers) and information based on them (biometric

information) are inherently "immutable." *Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1155 (7th Cir. 2020). COPPA, on the other hand, regulates "personal information," in the form of data-based identifiers. For instance, "personal information" includes one's name, physical and email addresses, telephone number, social security number, "persistent identifiers" like IP addresses and device serial numbers, and a person's geolocation information. 15 U.S.C. § 6501(8); 16 C.F.R. § 312.2. Indeed, BIPA's enactment was motivated, in large part, by this very distinction as shown in its legislative findings:

> ***17** Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, *social security numbers*, when compromised, *can be changed*. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

740 ILCS 14/5(c) (emphases added). The thematic difference between biology-based and data-based identifying information should be apparent. And considering these distinct regulatory targets, there is no basis to conclude that BIPA's requirements are "inconsistent" with COPPA's. *See H.K.*, 595 F. Supp. 3d at 711 (recognizing that "COPPA does not expressly reference biometric data in its statutory text.").

One form of "personal information" under COPPA does present a possible overlap with BIPA's regulation of biometric data: "A photograph, video, or audio file where such file contains a child's image or voice." 16 C.F.R. § 312.2. A child's "image" and "voice" are, of course, unique to them, and thus could trigger concomitant coverage under BIPA. But that alone is not enough to trigger preemption here. State laws that "supplement" or even "require the same thing" as federal law are not "inconsistent" with federal law. *Jones*, 73 F.4th at 642 (quotation marks and internal citations omitted).

Moreover, differences in regulatory methodologies do not justify preemption in this case because none of them involve the "inconsistent ... treatment" of a "photograph, video, or audio file where such file contains a child's image or voice." Meta has identified several requirements under COPPA that, it claims are "different[ ]" from BIPA's regulatory approach on similar matters. (Doc. 23 at 30-31 & n.16). First, 16 C.F.R. § 312.4(d) requires a website operator to "post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service." BIPA, on the other hand, requires an entity in possession of biometric data to "develop a written policy" for its retention and destruction and to "ma[k]e [the policy] available to the public." 740 ILCS 14/15(a). Meta argues that because BIPA does not require a policy that is "specific to children," its requirement that private entities publish their data retention and destruction policies is inconsistent with COPPA. This argument is easily rejected because a requirement that is silent on an issue that COPPA addresses can hardly be seen as "inconsistent" with it. Second, the FTC's regulations *allow* covered entities to retain personal information "as long as is reasonably necessary." *See* 16 C.F.R. § 312.10 (website operators "shall retain personal information collected online from a child for *only as long as is reasonably necessary* to fulfill the purpose for which the information was collected") (emphasis added). BIPA, however, *requires* the deletion of biometric data when the initial purpose for its collection is no longer present or three years after the subject's last interaction with the collecting entity. *See* 740 ILCS 14/15(a). This distinction is irrelevant for preemption purposes because there is no irreconcilable conflict between a federal law's grant of *permission* to do something (retain data) and a state law's *requirement* to eventually do the opposite (delete data). Third, Meta contends that COPPA's requirement that website operators obtain "verifiable parental consent" before collecting a child's personal information but allowing them to do so through "any reasonable effort," 16 C.F.R. § 312.2, is inconsistent with BIPA's requirement that private entities obtain a "written release" from people before collecting their biometric data. 740 ILCS 14/15(b)(3). Here too, there is no inconsistency. A federal statute that does not govern the form in which consent must be obtained is not inconsistent with a state law that does.

***18** The Court is equally unpersuaded that the lack of a private right of action under COPPA warrants the preemption of Plaintiffs' BIPA claims. The Seventh Circuit recognizes that "[t]he absence of a private right of action from a federal statute

provides no reason to dismiss a claim under a state law just because it refers to or incorporates some element of the federal law." *Wigod v. Wells Fargo Bank, N.A.*, 673 F.3d 547, 581 (7th Cir. 2012). Here, the two statutes occupy distinct regulatory fields with minimal (if any) substantive overlap. Thus, the absence of a private right of action provides no basis for a finding of "inconsistent" regulatory "treatment" that would trigger COPPA's preemption clause. 15 U.S.C. § 6502(d).

Based on the foregoing, the Court finds that Meta is unable to overcome the presumption against preemption in this case. *See Patriotic Veterans*, 736 F.3d at 1046. COPPA does not preempt Plaintiffs' BIPA claims with respect to Messenger Kids. It bars only the imposition of liability for covered conduct that is "inconsistent" with its treatment of such conduct. 15 U.S.C. § 6502(d). Nothing in sections 15(a) and 15(b) of BIPA impose such "inconsistent" requirements.

CONCLUSION

Meta's Motion to Dismiss Plaintiffs' complaint (Doc. 23) is **DENIED**. This case will proceed to discovery and the Court will set a telephonic scheduling conference by separate order.

IT IS SO ORDERED.

All Citations

Slip Copy, 2024 WL 4213302

Footnotes

1 Meta removed this case to federal court from the Circuit Court for the Twentieth Judicial Circuit, St. Clair County, Illinois. (Doc. 1 at 1). Thus, the allegations in Plaintiff's complaint and Meta's notice of removal serve as the basis for this Court's subject matter jurisdiction (Docs. 1 & 23-2). *See Dancel v. Groupon, Inc.*, 940 F.3d 381, 383-85 (7th Cir. 2019). Here, subject matter jurisdiction is secure under the Class Action Fairness Act ("CAFA"). *See* 28 U.S.C. § 1332(d). CAFA jurisdiction requires (i) the aggregate number of members in the proposed class to be 100 or more; (ii) the parties to be minimally diverse; and (iii) the matter in controversy to exceed $5,000,000, exclusive of interest and costs. *Id.* Plaintiffs' complaint alleges that the number of putative class members is in the "thousands" or even "millions." (Doc. 1 at 4). This satisfies the aggregate number requirement. Minimal diversity means that "any member of a class of plaintiffs is a citizen of a State different from any defendant." 28 U.S.C. § 1332(d)(2)(A). Here, the named Plaintiffs are citizens of Illinois, whereas Meta is a citizen of California and Delaware. (Docs. 1 at 2 & 1-3 at 2). This satisfies minimal diversity. Finally, BIPA provides for statutory damages of up to $5,000 per violation. *See* 740 ILCS 14/20(a)(2). With a putative class of "thousands or millions" of members, the $5,000,000 threshold is easily reached. This satisfies the amount in controversy requirement.

2 The statute excludes certain items from its definition of "biometric identifiers," including writing samples, photographs, descriptions of tattoos, descriptions of one's physical characteristics, and information and images generated for healthcare purposes. 740 ILCS 14/10. The excluded data types do not appear relevant here. *See In re Facebook Biometric Info. Priv. Litig.*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016) (statutory definition of "biometric identifier" "indicate[s] that the Illinois legislature enacted BIPA to address emerging biometric technology, such as Facebook's face recognition software ..., without including physical identifiers that are more qualitative and non-digital in nature.").

3 The duty to *publish* a data retention and destruction policy "is owed to the public generally, not to particular persons." *Bryant v. Compass Gr. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020). Individual plaintiffs thus do not have standing

to bring claims in federal court based solely on an entity's failure to publish a compliant policy. *Id.*; *Patterson*, 593 F. Supp. 3d at 802. An entity's failure to *comply with* its data retention and destruction policy, on the other hand, inflicts a particularized injury and allows individual plaintiffs to sue under section 15(a). *See Fox v. Dakkota Integrated Sys., LLC*, 980 F.3d 1146, 1154 (7th Cir. 2020) (plaintiff's allegation that defendant failed to "develop, publicly disclose, *and comply with* a data-retention schedule and guidelines for the permanent destruction of biometric data" sufficient to confer standing) (emphasis in original). Plaintiffs' claim under section 15(a) falls into the latter category. *See* Compl. at ¶¶ 145, 146 (Doc. 23-2) (alleging failure to "follow[ ]" retention schedule and destruction guidelines). Thus, it does not appear to pose any standing issues, nor has Meta raised any.

4 Meta also cites *Sonrai Sys., LLC v. AMCS Grp. Inc.*, No. 16 C 9404, 2017 WL 4281122, at *8 n.3 (N.D. Ill. Sept. 27, 2017), to argue that Exhibits D, E, G, and H should be considered under the incorporation-by-reference doctrine. But like *Gardner* and *James, Sonrai* is not a BIPA case, and its discussion of the doctrine is limited to a single footnote.

5 The Facebook Messenger Face and Hand Effects Privacy Notice (Exhibit C) contains nearly identical language to that in Messenger Kids' privacy notice (Exhibit B)—instead of referring to the user as "your child," it refers to the user as "you." (Doc. 23-3); *see also* (Doc. 23 at 12 n.2) (Meta's Motion to Dismiss explaining difference in wording between privacy notices).

6 Both documents contain the following copyright notice: "© 2023 Meta." (Docs. 23-3 & 23-4). This notice indicates 2023 as the year of first publication and identifies Meta as the owner of the copyrighted work. *See* 17 U.S.C. § 401(b) (outlining form and elements of copyright notice).

7 Meta's choice-of-law argument raises the important procedural issue of when and how to decide the case's governing law. The parties should give this question some thought because "the optimal timing for a choice-of-law determination is case-specific." *Foisie*, 967 F.3d at 42. Here, although the record does not permit an informed choice-of-law determination at this time, the issue may be a candidate for resolution on summary judgment. *See In re Facebook*, 185 F. Supp. 3d at 1159 (converting choice-of-law argument in motion to dismiss into summary judgment issue). The Court will address this and other matters at an upcoming scheduling conference.

8 The factual premise that Meta did not "collect" or "possess" the information at issue is based on documents that this Court has excluded from its review. Specifically, Meta points to language in Exhibits B and C (the Facebook Messenger and Messenger Kids Face and Hand Effects Privacy Notices) that states "[w]e [Meta] don't store this information on our servers or share it with third parties." (Docs. 23-3 at 2 & 23-4 at 2). To support its bid to have these documents considered, Meta cites *Zablocki v. Merchants Credit Guide Co.*, 968 F.3d 620, 623 (7th Cir. 2020), where the Seventh Circuit observed that "when the plaintiff relies on a document *attached to the complaint* and does not deny its accuracy, the facts communicated by that document control over allegations to the contrary" (emphasis added). In *Zablocki*, the plaintiffs attached certain documents to their complaint that had the unintended effect of negating a critical factual contention they made. *Id.* at 624. Here, Plaintiffs did not attach *any* documents to their complaint. Thus, Meta's exhibits are not susceptible to consideration in the same way the documents in *Zablocki* were. Moreover, to the extent that Plaintiffs cite Meta's claim that it does not store biometric data on its servers, they do so to *refute* its accuracy. *See* Compl. at ¶¶ 54 & 74 (Doc. 23-2) (noting Meta's "claim[ ]" that it does not store biometric data on its servers and refuting it by alleging the opposite). In other words, Plaintiffs openly contest the accuracy of the privacy notices, they do not acknowledge it. This distinguishes their invocation of the privacy notices from *Zablocki*, where the plaintiffs attached the documents at issue to their complaint and "d[id] not deny [their] accuracy." *Zablocki*, 968 F.3d at 623; *see also H.K. through Farwell v. Google LLC*, 595 F. Supp. 3d 702, 708 (C.D. Ill. 2022) ("Defendant's representations about its own privacy practices cannot control at the motion to dismiss stage.").

9 Meta has only raised express preemption as an affirmative defense. Thus, the Court will confine its analysis to that issue. *See Aux Sable*, 526 F.3d at 1033-34. It is worth noting, however, that conflict preemption and express preemption "effectively collapse into one when the preemption clause uses the term 'inconsistent,' " as COPPA's does. *Jones*, 73 F.4th at 644. Field preemption, moreover, is "rare" and requires a clear expression of congressional intent. *Nelson*, 928

F.3d at 651-52. Field preemption is unlikely here because "by expressly limiting federal preemption to state requirements that are *inconsistent* with the federal regulations, Congress signaled its intent not to occupy the entire field." *Metrophones Telecomms., Inc. v. Global Crossing Telecomms., Inc.*, 423 F.3d 1056, 1072 (9th Cir. 2005) (emphasis in original).

End of Document