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

ALEJANDRO MONROY, on behalf of himself and all others similarly situated,	)	
	)	Case No. 16 C 10984
Plaintiffs,	)	
	)	Judge Joan B. Gottschall
v.	)	
SHUTTERFLY, INC.,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

Alejandro Monroy ("Monroy") brings this putative class action alleging that defendant Shutterfly, Inc. ("Shutterfly") violated Illinois' Biometric Information Privacy Act (BIPA), 740 Ill. Comp. Stat. 14/1 *et seq*. Shutterfly has moved to dismiss the complaint on several grounds. For the reasons discussed below, the motion is denied.

I. BACKGROUND

Shutterfly is the operator of websites that allow users to upload, organize, and share digital photographs. When a user uploads a photo, Shutterfly's facial recognition software scans the image, locates each of the faces in the image, and extracts a highly detailed "map" or "template" for each face based on its unique points and contours. According to the complaint, a person can be uniquely identified by his face geometry in the same way that he can be identified by his fingerprints. Compl. ¶ 5.

The complaint further alleges that Shutterfly stores these maps of face geometry in a massive database, and that whenever a new image is uploaded onto Shutterfly's site, the faces in the image are compared against those in the database. If a face's geometry matches that of an

individual already in its database, Shutterfly suggests that the user "tag" the image with the individual's name. *Id*. ¶ 23. If no match is found, Shutterfly prompts the user to enter a name. *Id*.

Monroy alleges that in September 2014, an unnamed Shutterfly user residing in Chicago uploaded a photograph of Monroy onto a Shutterfly site. According to the complaint, "Shutterfly automatically located Plaintiff's face, analyzed the geometric data relating to the unique contours of his face and the distances between his eyes, nose and ears, and used that data to extract and collect Plaintiff's scan of face geometry." *Id*. ¶¶ 29-30. Monroy further says that Shutterfly prompted the uploader to tag the face with a name, and that the user entered "Alex Monroy." The complaint also states that Shutterfly then stored Monroy's biometric data in its database, and that based on the scan, it extracted and stored additional information regarding his gender, age, race, and geographical location. *Id*. ¶ 32. Monroy does not use Shutterfly and never consented to Shutterfly's extraction and storage of data representing his face geometry. *Id*. ¶¶ 33-34.

According to Monroy, Shutterfly's collection and storage of this data violates BIPA. Passed in 2008, BIPA was the first law in the nation to address the collection and storage of biometric data.[1] The legislative findings that precede the statute's substantive provisions observe that the "use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings." 740 Ill. Comp. Stat. 14/5(a). However, the legislature also notes that the "overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information." *Id*. § 14/5(d). This is because, unlike social security numbers and other personal information, biometrics "are biologically unique to the individual … [so that] once

[1] To date, Texas is the only other state to have passed a similar law. *See* Tex. Bus. & Com. Code Ann. § 503.001 (West 2015).

compromised, the individual has no recourse, [and] is at heightened risk for identity theft." *Id*. § 14/5(c).

Among other things, BIPA requires private entities in possession of biometric data to develop publicly available written policies containing guidelines for permanently destroying the data within a specific time period. *Id*. § 14/15(a). In addition, BIPA prohibits private entities from collecting, capturing, or otherwise obtaining an individual's biometric data without first informing him or her in writing, and disclosing the specific purpose and length of time for which the data is being collected and stored. *Id*. § 14/15(b)(1)-(2). Entities are prohibited from collecting and storing a person's biometric data unless he or she first executes a written release. *Id*. § 14/15(b)(3).

Monroy brings this suit on behalf of himself and a putative class consisting of "[a]ll individuals who are not users of Shutterfly and who had their biometric identifier, including scan of face geometry, collected, captured, received, or otherwise obtained by Shutterfly from a photograph uploaded to Shutterfly's website from within the state of Illinois." Compl. ¶ 36. Shutterfly moves to dismiss under Federal Rule of Civil Procedure 12(b)(6).

II. DISCUSSION

"In considering a Rule 12(b)(6) motion to dismiss, the Court accepts as true all well-pleaded facts in the complaint and draws all reasonable inferences from those facts in the plaintiff's favor." *United States Sec. & Exch. Comm'n v. Ustian*, 229 F. Supp. 3d 739, 760 (N.D. Ill. 2017) (citing *AnchorBank, FSB v. Hofer*, 649 F.3d 610, 614 (7th Cir. 2011)). Shutterfly claims that Monroy's complaint must be dismissed because: (1) BIPA's statutory text makes clear that it does not apply to scans of face geometry obtained from photographs; (2) Monroy's suit requires an impermissible extraterritorial application of the statute; and (3) BIPA requires a

plaintiff to allege actual damages, and Monroy has failed to do so. The court considers these arguments *seriatim*.

A. BIPA's Application to Scans from Photographs

Shutterfly first contends that BIPA's statutory text demonstrates that the act does not apply to biometric data obtained from photographs. Its argument is based on the statute's definitions of the terms "biometric identifier" and "biometric information," which are as follows:

> "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include 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. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.
>
> "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

740 Ill. Comp. Stat. 14/10.

It is clear that the data extracted from Monroy's photograph cannot constitute "biometric information" within the meaning of the statute: photographs are expressly excluded from the definition of "biometric identifier," and the definition of "biometric information" expressly

excludes "information derived from items or procedures excluded under the definition of biometric identifiers." *Id.*

But this leaves open the question of whether the data obtained from the photograph of Monroy may constitute a "biometric identifier"—and in particular, whether it constitutes a "scan of face geometry" referenced in the definition. Shutterfly maintains that by excluding data derived from photographs from the definition of "biometric information," the Illinois legislature intended to exclude from BIPA's purview all biometric data obtained from photographs. Accordingly, Shutterfly contends, it would make no sense to interpret "biometric identifier" as including such data.

This reading of the statute seems sensible enough at first blush, but it begins to unravel under scrutiny. Indeed, Google and Facebook have asserted the same argument in seeking dismissal of suits brought against them under BIPA, and in both cases, the argument has been rejected. *See, e.g.*, *Rivera v. Google Inc.*, No. 16 C 02714, 2017 WL 748590, at *6 (N.D. Ill. Feb. 27, 2017); *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1172 (N.D. Cal. 2016). The problems come more sharply into relief by considering what a "scan of face geometry" means under Shutterfly's interpretation of the statute. As Shutterfly acknowledges, if biometric identifiers do not include information obtained from images or photographs, the definition's reference to a "scan of face geometry" can mean only an *in-person* scan of a person's face. Such a narrow reading of the term "biometric identifier" is problematic in many respects. Foremost among these is the absence of any textual support for Shutterfly's interpretation. *See, e.g.*, *Rivera*, 2017 WL 748590, at *6 ("The problem with this argument is that there is no textual or structural clue to support it. The definition of 'biometric identifier' does not use words like 'derived from a person,' 'derived in person,' or 'based on an in-person scan,'

whereas the definition of 'biometric information' does say that it is information 'based on' a biometric identifier."); *In re Facebook*, 185 F. Supp. 3d at 1172 ("Trying to cabin this purpose within a specific in-person data collection technique has no support in the words and structure of the statute.").[2] The Illinois General Assembly clearly sought to define the term "biometric identifier" with a great deal of specificity: the definition begins by identifying six particular types of biometric data that are covered by the term (i.e., retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry); it then provides a long list of other specific types of biometric data that are excluded from the definition. If the legislature had intended a "scan of face geometry" to refer only to scans taken of an individual's actual face, it is reasonable to think that it would have signalled this more explicitly.

Shutterfly attempts to support its interpretation by invoking the canon of *noscitur a sociis*, according to which "the meaning of questionable words or phrases in a statute may be ascertained by reference to the meaning of words or phrases associated with it." *People v. Diggins*, 919 N.E.2d 327, 332 (Ill. 2009) (brackets and quotation marks omitted). According to Shutterfly, all of the other terms included in the definition of "biometric identifier"—retina or iris scans, fingerprints, voiceprints, and hand scans—involve "in-person processes." Hence, Shutterfly argues, a "scan of face geometry" should likewise be understood as referring only to data obtained from a person who is physically present. Shutterfly further contends that limiting

[2] In May 2016, Illinois State Senator Terry Link proposed an amendment that would have excluded both physical and digital photographs from BIPA's definition of "biometric identifier," and would have limited the definition of "scan" to in-person scans. *See* Natasha Kohne, Kamran Salour, *Biometric Privacy Litigation: Is Unique Personally Identifying Information Obtained from A Photograph Biometric Information?*, 25 Competition: J. Anti., UCL & Privacy Sec. St. B. Cal. 150, 165 (2016). The day after it was introduced, it was "put on hold" for unspecified reasons. *Id*. at 167.

the definition of "biometric identifier" to data obtained via in-person processes is consistent with the impetus behind BIPA's passage—namely, consumer wariness about the use of biometric data when making purchases and engaging in other commercial transactions. Further, Shutterfly points out that the examples cited in the legislative findings—"finger-scan technologies at grocery stores, gas stations, and school cafeterias" 740 Ill. Comp. Stat. 14/5(b)—take place in the consumer's physical presence.

For several reasons, the court is not persuaded. As an initial matter, Shutterfly's argument assumes that the other biometric identifiers listed in the definition can be obtained only via in-person processes. That is incorrect. For example, it appears that fingerprints and retinal scans can be obtained from images and photographs. *See, e.g.*, David Goldman, *Hackers Recreate Fingerprints Using Public Photos*, CNN MONEY (Dec. 30, 2014), http://money.cnn. com/2014/12/30/technology /security/fingerprint-hack/index.html (reporting a demonstration at a cybersecurity convention showing that it is possible to "mimic a fingerprint just by analyzing photographs"); Thomas Fox-Brewster, *Hacking Putin's Eyes: How to Bypass Biometrics the Cheap and Dirty Way with Google Images*, Forbes (Mar. 6, 2016), https://www. forbes.com /sites/thomasbrewster/ 2015/03/05/clone-putins-eyes-using-google-images/ #5cf7f79e214a) (reporting that, according to a security researcher, it is possible to fool iris-scanners "just using high-resolution images found in Google searches," and that "where photos are vivid and large enough, it's possible to simply print copies of people's eyes and bypass biometric authentication"); Kim Zetter, *Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners*, Wired (July 25, 2012), https://www.wired.com/2012/07/ reverse-engineering-iris-scans/(reporting that researchers in Spain have "found a way to recreate iris images that match digital iris codes that are stored in databases and used by iris-recognition systems to identify

people" and to "trick commercial iris-recognition systems into believing they're real images"). And even if particular forms of biometric data cannot be obtained via photographic images using present-day technology, it would be rash, given the pace of technological development, to assume that obtaining such data via photographs will not become possible in the future.

The court is also unconvinced by Shutterfly's insistence that BIPA is narrowly concerned with the use of biometric data in the context of commercial transactions. True, the statute's legislative findings observe that "[t]he use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings"; and that "[m]ajor national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions." 740 Ill. Comp. Stat. 14/5(a)-(b). But the legislative findings also take note of consumer leeriness regarding the connection between biometric data and personal information more generally. *See id.* § 14/5(d) (noting that "overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances *and other personal information*") (emphasis added). Nothing in the text of the law itself evinces an intent to limit its application to commercial entities. On the contrary, the law applies to any "private entity" in possession of biometric data; and the statute's definition of "private entity" is notably expansive, encompassing "any individual, partnership, corporation, limited liability company, association, or other group, however organized." *Id.* § 14/10.

Finally, as other courts have observed, the interpretation of the term "scan of face geometry" proposed by Shutterfly would leave little room for the law to adapt and respond to technological development. BIPA's legislative findings specifically note that "[t]he full ramifications of biometric technology are not fully known." *Id.* § 14/5(f). As Judge Chang stated

in *Rivera*, "advances in technology are what drove the Illinois legislature to enact the Privacy Act in the first place," so "it is unlikely that the statute sought to limit the definition of biometric identifier by limiting how the measurements are taken. Who knows how iris scans, retina scans, fingerprints, voiceprints, and scans of faces and hands will be taken in the future?" 2017 WL 748590, at *5; *see also In re Facebook*, 185 F. Supp. 3d at 1172 ("The statute is an informed consent privacy law addressing the collection, retention and use of personal biometric identifiers and information at a time when biometric technology is just beginning to be broadly deployed. Trying to cabin this purpose within a specific in-person data collection technique has no support in the words and structure of the statute, and is antithetical to its broad purpose of protecting privacy in the face of emerging biometric technology.") (citation omitted).[3]

[3] Shutterfly also cites BIPA's legislative history in support of its interpretation of "biometric identifier." Specifically, Shutterfly observes that an earlier version of the definition stated: "'Examples of biometric identifiers include, *but are not limited to*[,] iris or retinal scans, fingerprints, voiceprints, and *records* of hand or facial geometry." Defs.' Br. 8 (quoting Sen. Bill 2400, § 10 (Feb. 14, 2008)) (emphasis supplied by Shutterfly). Shutterfly also notes that the Illinois Senate considered and rejected a proposal that would have defined "biometric identifier" to include "'records or scans of hand geometry, facial geometry, or *facial recognition*.'" *Id*. (quoting Sen. Am. to Sen. Bill 2400, § 10 (Apr. 11, 2008)) (emphasis supplied by Shutterfly). Finally, Shutterfly points out that an earlier definition of "biometric information" did not include the clause stating that "[b]iometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers," 740 Ill. Comp. Stat. 14/10, and thus did not exclude data derived from photographs.

Shutterfly reasonably regards these textual changes as evidence of the legislature's attempts to limit the definition of "biometric identifier." However, they provide no evidence that the legislature intended to confine the term "scans of face geometry" to data obtained in person, nor that it intended to exclude data obtained from photographs from the definition of "biometric identifier." If anything, Shutterfly's position is significantly undermined by its failure to identify any reference in the legislative record to in-person processes or any distinction between biometric data obtained by such processes and data obtained from digital images and other sources.

In short, the court sees nothing in BIPA's statutory text to indicate that it lacks application to data of the sort obtained by Shutterfly's facial-recognition technology.

B. Extraterritoriality & The Dormant Commerce Clause

Turning from BIPA's text to its application, Shutterfly next argues that Monroy's complaint must be dismissed because BIPA does not apply extraterritorially, and because applying the statute to the facts of this case would violate the U.S. Constitution's Dormant Commerce Clause. Although related, these arguments raise separate concerns, and the court addresses them separately.

1. Extraterritoriality

The Illinois Supreme Court has stated that "a 'statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute.'" *Avery v. State Farm Mut. Auto. Ins. Co*., 835 N.E.2d 801, 852 (2005) (quoting *Dur–Ite Co. v. Industrial Comm'n*, 68 N.E.2d 717 (1946)). However, none of BIPA's express provisions indicates that the statute was intended to have extraterritorial effect. Accordingly, as Monroy acknowledges, BIPA does not apply extraterritorially.

However, the parties disagree over whether Monroy's suit in fact requires the statute's extraterritorial application. The answer to that question turns on whether "the circumstances that relate to the disputed transaction occur[red] primarily and substantially in Illinois." *Id.* at 854.[4]

[4] *Avery* involved the question of whether the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505/2, applied extraterritorially. Hence, in the passage quoted above, the court is concerned with the location of the circumstances surrounding the disputed "transaction." However, *Avery*'s extraterritoriality test has been applied to other Illinois statutes. *See, e.g., Armada (Singapore) Pte Ltd. v. Amcol Int'l Corp.*, No. CV 13 C 3455, 2017 WL 1062322, at *5 (N.D. Ill. Mar. 21, 2017) (applying *Avery* to claim under Illinois Uniform Fraudulent Transfer Act); *Rivera*, 238 F. Supp. 3d at 1102 (applying *Avery* to claim under BIPA). Hence, like the parties, the court relies on *Avery* in determining whether Monroy's suit requires BIPA's extraterritorial application.

There "is no single formula or bright-line test for determining whether a transaction occurs within [Illinois]." *Id*. Rather, "each case must be decided on its own facts." *Id*.

Here, some of the circumstances relating to Monroy's suit are alleged to have occurred in Illinois: the complaint alleges that the photo of Monroy was uploaded to Shutterfly's website from a device that was physically located in Illinois and had been assigned an Illinois-based IP address. Compl. ¶ 10. Monroy also alleges that the photo was uploaded by a citizen of Illinois. *Id*. ¶ 29. In addition, he maintains that the actual violation of the statute took place in Illinois because that is where Shutterfly failed to obtain the requisite release prior to allegedly collecting his biometric data. At the same time, other relevant circumstances point to locations outside of Illinois: Monroy himself is a citizen and resident of Florida, and Shutterfly is a Delaware corporation headquartered in California. Moreover, Shutterfly argues while Monroy claims that the alleged violation took place in Illinois, he does not claim to have suffered any injury in Illinois.

However, the location of other important circumstances is as yet undetermined. For example, it is unclear where the actual scan of Monroy's face geometry took place, and where the scan was stored once it was obtained. Answers to these questions require a fuller understanding of how Shutterfly's facial recognition technology operates. In addition, these factual questions potentially raise legal questions that the parties have not addressed. (For example, given that Monroy's biometric data was extracted and stored in cyberspace, how is their physical location to be determined?).

In short, the court is unable at this time to determine whether the circumstances of Monroy's claim can be said to have occurred primarily and substantially in Illinois, and thus whether Monroy's suit would require extraterritorial application of BIPA. At this stage,

therefore, the court is not persuaded by Shutterfly's extraterritoriality argument. Shutterfly may raise the argument at a later time, if and when the record affords a clearer picture of the circumstances relating to Monroy's claim. *See Rivera*, 2017 WL 748590, at *10 ("Assessing [the defendant's extraterritoriality] arguments at this initial stage, the Court concludes that the Plaintiffs sufficiently allege facts that would deem the asserted violations as having happened in Illinois. But there is no bright-line rule for determining this, so the parties will have the chance to develop more facts during discovery.").

2. The Dormant Commerce Clause

Shutterfly also argues that BIPA's application to the facts of this case would violate the Dormant Commerce Clause. While the Constitution "explicitly grants Congress the authority to regulate commerce among the States, it has long been understood that it also directly limits the power of the States to discriminate against or burden interstate commerce." *Alliant Energy Corp. v. Bie*, 330 F.3d 904, 911 (7th Cir. 2003). "This 'negative' aspect of the Commerce Clause is often referred to as the 'Dormant Commerce Clause' and is invoked to invalidate overreaching provisions of state regulation of commerce." *Id.*

Shutterfly correctly observes that the Dormant Commerce Clause "precludes the application of a state statute" that has "the practical effect of . . . control[ling] conduct beyond the boundaries of the State," "whether or not the commerce has effects within the State"—thereby preventing "inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." Def.'s Br. 12 (quoting *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 336-37 (1989)). According to Shutterfly, applying BIPA in this case would have precisely these effects. This is especially problematic, Shutterfly argues, because California, where it is headquartered, previously rejected legislation that would have regulated the collection

and storage of biometric data. *See* Def.'s Br. 13 (citing Cal. Sen. Bill No. 169 (July 5, 2001) (Ex. E)); *see also* Yana Welinder, *A Face Tells More Than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 Harv. J.L. & Tech. 165, 200 (2012) (describing a bill that did not pass at the end of the 2011-2012 legislative session that "would have required a company that collects or uses 'sensitive information,' including biometric data, to allow users to opt out of its collection, use, and storage"). Thus, Shutterfly contends that to apply BIPA to these facts would be to override California's decision against regulating biometric data.

This contention is overwrought. Shutterfly cites three cases in support of its position: *Morrison v. YTB International, Inc.*, 649 F.3d 533 (7th Cir. 2011), *Midwest Title Loans, Inc. v. Mills*, 593 F.3d 660 (7th Cir. 2010), and *Morley-Murphy Co. v. Zenith Electronics Corp.*, 142 F.3d 373 (7th Cir. 1998). The laws at issue in these cases affected out-of-state conduct in a very different way, and to a very different degree, than would result from applying BIPA in this case. *Midwest Title*, for example, struck down an Indiana law purporting to regulate car-title loans to Indiana citizens, even when the loan transactions took place in other states. *Id*. at 669. *Morley-Murphy* addressed whether the Wisconsin Fair Dealership Law could be invoked to prevent manufacturers from terminating their relationships with distributors, even where neither party was located in Wisconsin. *Id*. at 378-80. *Morrison v. YTB Int'l, Inc*., 649 F.3d 533 (7th Cir. 2011), did not mention the commerce clause at all, but simply observed that "[e]xpanding Illinois law in a way that overrode the domestic policy of other states would be problematic." *Id*. at 538.

Monroy's suit, as well as his proposed class, is confined to individuals whose biometric data was obtained from photographs uploaded to Shutterfly in Illinois. Applying BIPA in this case would not entail any regulation of Shutterfly's gathering and storage of biometric data obtained outside of Illinois. It is true that the statute requires Shutterfly to comply with certain

regulations if it wishes to operate in Illinois. But that is very different from controlling Shutterfly's conduct in other states. Indeed, laws imposing similar requirements on out-of-state businesses have been upheld against Dormant Commerce Clause challenges. In *International Dairy Foods Ass'n v. Boggs*, 622 F.3d 628 (6th Cir. 2010), for example, the Sixth Circuit rejected a Dormant Commerce Clause challenge brought by out-of-state dairy processors to an Ohio law requiring the inclusion of certain information on the labels of milk products sold within the state. Similarly, in *National Electrical Manufacturers Ass'n v. Sorrell*, 272 F.3d 104 (2d Cir. 2001), the Second Circuit rejected a Dormant Commerce Clause challenge by out-of-state manufacturers to a Vermont statute imposing labeling requirements for lamps containing mercury sold within the state.

As noted above, important information is lacking regarding how Shutterfly's technology works. It is therefore conceivable that, after further development of the factual record, this case will appear closer to *Midwest Title* than to *Boggs* or *Sorrell*. At this point, however, the court has no basis for concluding that applying BIPA in this case would entail control over out-of-state conduct in a way that would run afoul of the dormant commerce clause. *Cf. Rivera*, 2017 WL 748590, at *12 ("The Commerce Clause argument is directly related to the extraterritoriality effect argument…. Whether [BIPA] is nevertheless being summoned here to control commercial conduct wholly outside Illinois is not possible to figure out without a better factual understanding of what is happening in the Google Photos face-scan process. What is learned from discovery there will inform both the more general extraterritoriality analysis above and this Dormant Commerce Clause analysis.").

For these reasons, the court is unpersuaded at this stage that Monroy's suit requires BIPA's application extraterritorially or in a way that violates the Dormant Commerce Clause.

C. Actual Damages

As a final basis for dismissal of Monroy's suit, Shutterfly argues that Monroy has failed to allege that he suffered actual damages as a result of Shutterfly's conduct. Monroy responds that it is unnecessary to allege actual damages to state a claim under BIPA, but that, in any event, he has alleged actual damage by claiming that Shutterfly invaded his privacy. This raises two questions: (1) whether BIPA requires a plaintiff to allege actual damages; and if so (2) whether Monroy has sufficiently alleged such damages.

BIPA's text is of little help in answering these questions. The statute does not define the meaning of "actual damages." The term is mentioned only in § 14/20(1), which provides: "A prevailing party may recover for each violation: (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater." 740 Ill. Comp. Stat. 14/20(1). To date, few courts have addressed whether BIPA requires a showing of actual damages, and those that have pronounced on the issue have reached opposite conclusions. *Compare Rosenbach v. Six Flags Entertainment Corp.*, 2016 CH 13 (Cir. Ct., Lake County, Ill., June 17, 2016) (BIPA does not require a showing of actual damages), with *Rottner v. Palm Beach Tan, Inc.*, No. 2015-CH-16695 (Ill. Cir. Ct. Dec. 20, 2016) (BIPA requires a showing of actual damages). Nor does the term otherwise have a settled meaning. *See, e.g., F.A.A. v. Cooper*, 566 U.S. 284, 294 (2012) (observing that "the term 'actual damages' has this chameleon-like quality," and that while in some contexts it has been "construed … narrowly to authorize damages for only pecuniary harm," in other contexts is has been "understood to include nonpecuniary harm"). Monroy argues that, read straightforwardly, § 14/20(1) presents plaintiffs with "a binary election between actual or statutory liquidated damages." Pl.'s Resp. Br. 23. According to Shutterfly, recovery under BIPA always requires a showing of actual damages.

The option of liquidated damages exists under § 14/20(1) solely for cases in which a plaintiff's actual damages cannot reliably be quantified.

Although the question is a close one, the court ultimately is not persuaded by Shutterfly's position. Shutterfly's argument is based on cases in which courts have interpreted other statutes to require a showing of actual damages.[5] But each of these cases is readily distinguishable. For

[5] In *McCollough v. Smarte Carte, Inc.*, No. 16 C 03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016), the court opined that actual damages were required to state a claim under BIPA. However, *McCollough*'s treatment of the issue came only after the court had concluded that, based on the plaintiff's failure to allege a concrete injury-in-fact, the suit had to be dismissed for lack of Article III standing. *Id*. at *4. Further, in stating that BIPA required a showing of actual-injury, the court relied heavily on *Doe v. Chao*, 540 U.S. 614 (2004), and *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535 (7th Cir. 2012). As is discussed more fully below, the court concludes that these cases are inapposite here.

The court notes that, in addition to *McCollough*, *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499 (S.D.N.Y. 2017), also dismissed a BIPA suit after concluding that the plaintiffs were unable to satisfy Article III's injury-in-fact requirement. Although Shutterfly has not challenged Monroy's standing in this case, the court has an independent obligation to assure itself of its jurisdiction. *See, e.g.*, *Baez-Sanchez v. Sessions*, 862 F.3d 638, 641 (7th Cir. 2017). The court has considered the issue and has concluded that Monroy has alleged a sufficient injury-in-fact for Article III purposes. Putting aside the question of whether a merely procedural or technical violation of the statute alone is sufficient to confer standing in light of *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), Monroy alleges that Shutterfly has violated his right to privacy. As courts have noted in discussing the issue of standing in the context of other statutes designed to safeguard privacy, "[a]ctions to remedy defendants' invasions of privacy … have long been heard by American courts, and the right of privacy is recognized by most states." *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017); *Pavone v. Law Offices of Anthony Mancini, Ltd.*, No. 15 C 1538, 2016 WL 7451628, at *2 (N.D. Ill. Dec. 28, 2016) ("[A] violation of the right to privacy results in the sort of harm that provides an appropriate basis for a lawsuit."). In this respect, the facts alleged in this case differ significantly from those alleged in *McCollough* and *Vigil*. In the latter cases, the plaintiffs voluntarily provided their biometric data to the defendants. The plaintiff in *McCollough* had rented one of the defendant's electronic storage lockers, which were locked and unlocked using customers' fingerprints on a touchscreen. In *Vigil*, the plaintiffs voluntarily had their faces scanned to create personalized avatars for use in a videogame. The harm alleged in the latter cases was the defendants' failure to provide them with certain disclosures (e.g., that their biometric data would be retained for a certain length of time after it had been obtained). Monroy, by contrast, alleges that he had no idea that Shutterfly had obtained his biometric data in the first place. Thus, in addition to any violation of BIPA's disclosure and informed consent requirements, Monroy also credibly alleges an invasion of his privacy.

example, *Doe v. Chao*, 540 U.S. 614 (2004), held that plaintiffs were required to show actual damages in order to recover under the Privacy Act of 1974, 5 U.S.C. § 552a(b). However, the provision at issue in *Doe* made the government liable for violations in the amount of the "actual damages sustained by the individual as a result of the [violation], but in no case shall a person entitled to recovery receive less than the sum of $1,000." *Doe*, 540 U.S. at 619 (quoting 5 U.S.C. § 552a(g)(4)(A)). Whereas § 14/20(1) presents liquidated damages and actual damages disjunctively, the reference to statutory damages in the Privacy Act is more naturally read as placing a lower limit on the amount of a plaintiff's recovery. Moreover, the plaintiff in *Doe* sued based on a specific provision of the Privacy Act that applied where violation of the act had resulted in an "adverse effect on an individual." *See* 5 U.S.C. § 552a(g)(1)(D) (providing a cause of action where the government "fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual"). Thus, under the provision in question, a plaintiff must show some form of actual harm even before the statutory damages provision comes into play. *Id*. at 620. Here, by contrast, nothing in BIPA makes recovery dependent upon a showing of "adverse effects."

Similarly, *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535 (7th Cir. 2012), held that plaintiffs are required to show actual damages in order to recover under the federal Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710. Like the Privacy Act in *Doe*, the VPPA provides for recovery of "actual damages but not less than liquidated damages in an amount of $2,500," 18 U.S.C. § 2710(c)(2)(A), and thus can be read as establishing a lower limit on the amount of a plaintiff's recovery, rather than as an alternative type of recovery. Moreover, as was also true in *Doe*, *Sterk*'s conclusion was based in key part on idiosyncratic aspects of the VPPA's structure. Specifically, the court noted that although the statute included multiple subsections

outlining various prohibitions—e.g., wrongful disclosure of private information, § 2710(b); receipt of such information as evidence in a legal, regulatory, or arbitral proceeding, § 2710(d); failure to destroy private information in a timely manner, § 2710(e)—the provision creating a private cause of action, § 2710(c), was inserted immediately after subsection (b), which prohibited the wrongful disclosure of information. Hence, the court concluded that Congress had intended to make recovery available only in cases where private information was wrongfully disclosed. Once again, this structural peculiarity is absent from BIPA. Rather, § 14/20(1) applies to "[a]ny person aggrieved by a violation of th[e] Act."

Finally, Shutterfly cites *Pace Communications, Inc. v. Moonlight Design, Inc.*, 31 F.3d 587 (7th Cir. 1994), for the proposition that a liquidated damages "provision must be a reasonable attempt to estimate actual damages." *Id.* at 593. But the question presented in *Pace Communications* was whether the liquidated damages provision in the parties' contract was enforceable. The court held that such provisions are enforceable only if they are reasonable. Nothing in the decision suggests that liquidated damages can never serve any function other than to provide an estimate of actual damages.

Moreover, in contrast to the statutes in *Doe* and *Sterk*, the court notes that many statutes have been interpreted as allowing recovery of statutory damages without a showing of actual damages. These include the Fair Credit Reporting Act, *see, e.g.*, *Murray v. New Cingular Wireless Servs., Inc.*, 232 F.R.D. 295, 303 (N.D. Ill. 2005) ("Proof of actual damage is not required to state a cause of action under the provision at issue here. Murray only has to show that the prescreening of the proposed class's credit did not comport with any of the permissible purposes outlined in section 1681b [of the FCRA]."); the Fair Debt Collection Practices Act, *see, e.g.*, *Keele v. Wexler*, 149 F.3d 589, 593 (7th Cir. 1998) ("The FDCPA does not require proof of

actual damages as a precursor to the recovery of statutory damages."); and the Truth in Lending Act, *see, e.g.*, *Brown v. Marquette Sav. & Loan Ass'n*, 686 F.2d 608, 614 (7th Cir. 1982) ("[T]he violation before us is a purely technical one, and that the plaintiffs do not claim that they were misled or suffered any actual damages as a result of the statutory violation. It is well settled, however, that a borrower need not have been so deceived to recover the statutory penalty."). In short, while the matter is not free from doubt, the court declines to hold that a showing of actual damages is necessary in order to state a claim under BIPA.

In light of this conclusion, the court need not address the question of whether, in alleging that Shutterfly invaded his privacy, Monroy has in fact alleged that he suffered a form of actual damage. The court notes, however, that Shutterfly has failed to address this issue. Instead, it asserts that Monroy's argument "can be disregarded because plaintiff's complaint does not claim that he suffered these damages." Def.'s Reply Br. 18. That is not true. Monroy specifically alleges that "[b]y collecting, storing, and using Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Shutterfly violated the right of Plaintiff and each Class member to privacy in their biometric identifiers and biometric information." Compl. ¶ 51.

Thus, the court declines to dismiss Monroy's suit based on his alleged failure to allege actual damges.

CONCLUSION

For the reasons discussed above, Shutterfly's motion to dismiss, ECF No. 22, is denied.

Date: Sept. 15, 2017

/s/

Joan B. Gottschall
United States District Judge