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

LINDABETH RIVERA and JOSEPH WEISS, on behalf of themselves and all others similarly situated,	)	
Plaintiffs,	)	No. 16 C 02714
v.	)	
	)	Judge Edmond E. Chang
GOOGLE, INC.,	)	
Defendant.	)	

MEMORANDUM OPINION AND ORDER

Under the Illinois Biometric Privacy Act, a private entity cannot collect or store certain kinds of biometric information, including face-geometry scans, without first obtaining consent or providing certain disclosures. 740 ILCS 14/1 *et seq*. Plaintiffs Lindabeth Rivera and Joseph Weiss both allege that Google unlawfully collected, stored, and exploited their face-geometry scans via Google Photos, a cloud-based service.[1] R. 63, Second Am. Compl. ¶¶ 4-5, 28-30, 33-36, 38-39, 42-45, 57-60, 67-70;

[1]The Court has diversity jurisdiction over Rivera's and Weiss's state-law claims under 28 U.S.C. § 1332. Rivera and Weiss are citizens of Illinois. R. 63, Second Am. Compl. ¶¶ 7-8. Google is a citizen of Delaware (its place of incorporation) and California (its principal place of business). *Id.* ¶ 9. Although Google, Inc. has since reorganized from a corporation to a limited liability company, FCC Report. No. SCL-00205 (Nov. 24, 2017), "the jurisdiction of the court depends upon the state of things at the time of the action brought," *Grupo Dataflux v. Atlas Glob. Grp., L.P.*, 541 U.S. 567, 570 (2004) (quotation omitted).

The amount in controversy requirement is also satisfied. The aggregate claims of the potential class (which would number in the thousands of members) could possibly equal or exceed $5,000,000, exclusive of interest and costs. 28 U.S.C. § 1332(d)(6). Even setting aside the class allegation, it is not "legally impossible" for either Weiss or Rivera alone to recover more than $75,000 in this action. *Back Doctors Ltd. v. Metro. Prop. & Cas. Ins. Co.*, 637 F.3d

see also R. 167, Pl.'s Resp. Br. at 1-3.[2] Google now moves for summary judgment on all of Plaintiffs' claims against it, arguing that Plaintiffs cannot establish Article III standing; Plaintiffs are not "aggrieved" within the meaning of the Act; and Plaintiffs are not entitled to monetary or injunctive relief under the Act because they have suffered no harm.[3] R. 151, Def.'s Mot. Summ. J.

For the reasons discussed below, Plaintiffs have not suffered an injury sufficient to establish Article III standing and their claims are dismissed. Because the Court lacks subject matter jurisdiction over Plaintiffs' claims, the Court need not consider Google's other arguments.

I. Background

In deciding Google's motion for summary judgment, the Court views the evidence in the light most favorable to Plaintiffs, the non-moving parties. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986). Google Photos is a free, cloud-based service for organizing and sharing photographs. R. 153, Def. SOF ¶ 7; R. 167-1, Pls. Resp. Def. SOF ¶ 10. When a user uploads a photo to Google Photos, Google Photos detects images of faces, then creates a face template, represented by [redacted]

827, 830 (7th Cir. 2011) (amount-in-controversy requirement satisfied unless it is "legally impossible" for a plaintiff to recover that amount).

[2]Citations to the record are noted as "R." followed by the docket number and the page or paragraph number.

[3]The parties agreed to defer argument on and resolution of other issues, such as liability under the Act (whether face templates qualify as "biometric identifiers" or "biometric information" under the Act, and whether Google provided sufficient disclosures or obtained sufficient consent), Google's defense under the Dormant Commerce Clause, whether the Act applies extraterritorially, and choice of law. R. 137, Joint Status Report 03/28/18; *see also* R. 152, Def.'s Br. at 4 n.2. Where relevant, the Court will note when it is assuming certain facts in favor of Plaintiffs for the purposes of this Opinion, even though Google has not conceded the issue outside of the motion under consideration.

[redacted]. Def. SOF ¶¶ 13-15. Google uses these face templates to compare the visual similarity of faces within Google Photos users' private accounts, *id.* ¶ 15, and then groups photographs with visually similar faces and displays the groups (called "face groups") to the users' private account, *id.* ¶ 9. Google Photos' face-recognition feature automatically defaults to "on" and is applied to every photo uploaded to the service unless the user opts out. Pls. Resp. Def. SOF ¶¶ 8, 10. The technology also can be applied to photos on the user's phone if "Private Face Clustering" is enabled. *Id.* ¶ 10. Google Photos users can assign a label (for example a name or title) to any face groups in their private accounts. Def. SOF ¶ 18. These face labels are private to individual users' accounts and are visible only to that user and to Google.[4] *Id.* ¶ 20. Google does not use the face templates it creates for anything other than organizing photographs in users' Google Photos accounts.[5] *Id.* ¶ 59.

[4]Plaintiffs dispute this, contending that "[l]abels, face templates, and all associated data in Google Photos are accessible to Google, its personnel, and to any party that Google permits to access such data." Pls. Resp. Def. SOF ¶ 20 (citing R. 153-3, Porter Decl. ¶¶ 4-10). But Porter's declaration states that the Plaintiffs' face templates are private to their accounts, and that the labeled face group of Rivera has not been "disclosed to anyone outside of Google." Porter Decl. ¶¶ 6-7. And Plaintiffs do not dispute that "[t]here is no evidence that the … face labels from the photographs of [Plaintiffs] … have been shared outside of Google." Pls. Resp. Def. SOF ¶ 52. There is no genuine dispute of material fact that face labels are visible only to the user and Google.

[5]Plaintiffs also dispute this, and argue that "the facial recognition … can be monetized by Google." Pls. Resp. Def. SOF ¶ 59; R. 167-1, Pls. Statement Add. Facts ¶ 6. As discussed in more depth below, the only evidence offered by Plaintiffs shows that Google *might* use this technology to mine data or target advertisements in the *future*. Pls. Resp. Def. SOF ¶ 59; Pls. Statement Add. Facts ¶ 6. Although that sort of use without obtaining the proper consent might very well constitute a concrete injury, Plaintiffs provide no evidence that Google has engaged in those practices with respect to Plaintiffs' face templates or photographs.

Weiss is a Google Photos user, Def. SOF ¶ 24, and the face-grouping feature in his account was defaulted to "on" until he turned it off sometime in mid-December 2017, Pls. Resp. Def. SOF ¶ 25. There are 53 photographs of Weiss that form the basis of his claim. Def. SOF ¶ 26. At least 16 of them were taken after he filed his complaint on March 4, 2016, but before he turned off the face-grouping feature. *Id.* ¶ 27. Weiss's Google Photos account, which is associated with his face template, is also associated with his Gmail account. Pls. Resp. Def. SOF ¶ 53. On the other hand, Rivera is not a Google Photos user, Def. SOF ¶ 31, but her friend Blanca Gutierrez is,[6] *id.* ¶¶ 32-33. The face-grouping feature was defaulted to "on" in Gutierrez's Google Photos account. Pls.' Resp. Def. SOF ¶ 34. There are at least 27 photos of Rivera taken by Gutierrez and uploaded to Gutierrez's Google Photos account that form the basis for Rivera's claim. *Id.* ¶¶ 35-36. At least 10 of the photographs of Rivera uploaded to Gutierrez's Google Photos account were taken after Rivera filed her complaint. Def. SOF ¶ 38. Gutierrez labeled a face group in her account as "LindaBeth Rivera." *Id.* ¶ 44. Apart from Weiss's Gmail account and Gutierrez's labelled face group, Plaintiffs' face templates are not associated with other identifying information, such as their social security numbers or credit card information. Pls. Resp. Def. SOF ¶¶ 53-54. Google did not have permission from Plaintiffs to capture, store, or use face scans of Plaintiffs.[7] Pls. Statement Add. Facts ¶ 2.

[6]Ms. Gutierrez is not a party to this action. Def. SOF ¶ 32.

[7]Google disputes whether it obtained consent or provided notice in compliance with the Act, 740 ILCS 14/15. R. 179-1, Def. Resp. Pls. Statement Add. Facts ¶ 2. As noted earlier, resolution of that issue was deferred to after the resolution of this motion. *Id.*; Joint Status Report 03/28/18. For the purposes of this motion, the Court assumes that Google did not obtain sufficient consent.

Weiss and Rivera both claim injury to their privacy interests, but testified that they did not suffer any financial, physical, or emotional injury apart from feeling offended by the unauthorized collection. R. 179-1, Def. Resp. Pls. Statement Add. Facts. ¶¶ 3-4. Weiss testified that he would not have given consent to collect his face template if Google had asked him to do so, although he was not sure if he would have stopped using Google Photos altogether. Pls. Resp. Def. SOF ¶ 29. The face templates and face groups associated with Weiss's and Gutierrez's Google Photos accounts are private, and there is no evidence of any unauthorized access into the accounts. Def. SOF ¶¶ 49-50.

II. Standard

Summary judgment must be granted "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). A genuine issue of material fact exists if "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). In evaluating summary judgment motions, courts must view the facts and draw reasonable inferences in the light most favorable to the non-moving party. *Scott v. Harris*, 550 U.S. 372, 378 (2007). The Court may not weigh conflicting evidence or make credibility determinations, *Omnicare, Inc. v. UnitedHealth Grp., Inc.*, 629 F.3d 697, 704 (7th Cir. 2011), and must consider only evidence that can "be presented in a form that would be admissible in evidence." Fed. R. Civ. P. 56(c)(2). The party seeking summary judgment has the initial burden of showing that there is no genuine dispute

and that they are entitled to judgment as a matter of law. *Carmichael v. Village of Palatine*, 605 F.3d 451, 460 (7th Cir. 2010); *see also Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986); *Wheeler v. Lawson*, 539 F.3d 629, 634 (7th Cir. 2008). If this burden is met, the adverse party must then "set forth specific facts showing that there is a genuine issue for trial." *Anderson*, 477 U.S. at 256.

III. Analysis

Google argues that this Court lacks subject matter jurisdiction over this case because Plaintiffs have not shown they have suffered concrete injuries sufficient to satisfy Article III standing, and even if Plaintiffs could establish concrete injuries, those injuries were not caused by Google's conduct. Standing requires that a plaintiff "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (citations omitted). Predictably, the parties dispute how the Court should apply the Supreme Court's most recent pronouncement on the injury-in-fact requirement, *Spokeo v. Robins*, so it is worth examining that opinion before delving into the facts of this case.

A. *Spokeo*

A plaintiff can, in some instances, satisfy the concrete-injury requirement of Article III absent actual monetary damages. But in those cases, federal courts must carefully ensure that the concrete-injury requirement is still met. In *Spokeo*, the plaintiff alleged that an online personal-information publisher violated the Fair Credit Reporting Act by publishing inaccurate information about him. 136 S. Ct. at

1546. The website got several things wrong, incorrectly reporting that "he is married, has children, is in his 50's, has a job, is relatively affluent, and holds a graduate degree." *Id.* But despite these mistakes, the plaintiff did not allege that he suffered any actual monetary harm. *Id.* at 1546, 1550. Even without that allegation, the Supreme Court reiterated that the concrete-injury requirement can be satisfied even if the injury is not tangible. *Id.* at 1549. The Court explained, "[a]lthough tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that *intangible* injuries can nevertheless be concrete." *Id.* (emphasis added).[8]

In determining which intangible injuries are sufficient to confer standing and which are not, *Spokeo* set out basic principles: a "bare procedural violation" of a statute is *not* automatically enough to satisfy Article III's concreteness requirement. 136 S. Ct. at 1549. To be sure (and as Plaintiffs here discuss in detail), "[i]n determining whether an intangible harm constitutes injury in fact, both history and the judgment of Congress play important roles." *Id.* When Congress has created a cause of action for a statutory violation, by definition it has created a legally protected interest that Congress, at least, deems important enough for a lawsuit. Going beyond *federal* statutes, the Seventh Circuit has recognized the importance of state legislative judgments as well. *See Scanlan v. Eisenberg*, 669 F.3d 838, 845 (7th Cir. 2012) (noting the importance of federal congressional judgments and reasoning "the

[8]At the same time, concreteness is indeed a requirement that is separate and apart from the Article III requirement that the injury be "particularized" to the individual plaintiff. *Spokeo*, 136 S. Ct. at 1548. Specifically, "[t]o establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete *and* particularized.'" *Id.* at 1548 (emphasis added) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)).

same must also be true of legal rights growing out of state law") (cleaned up).[9] *Spokeo* explained that the legislative branch, with its fact-finding ability and responsiveness to public interest, "is well positioned to identify intangible harms that meet minimum Article III requirements," so Congress's (or the state legislature's) judgment on the nature of the injury is "instructive and important." 136 S. Ct. at 1549. Still, "Congress' role in identifying and elevating intangible harms does *not* mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right … . Article III standing requires a concrete injury even in the context of a statutory violation." *Id.* (emphasis added).

Spokeo also announced the principle that the *risk* of harm sometimes is enough to satisfy concreteness. 136 S. Ct. at 1549. To illustrate this point, the Supreme Court offered both a historical example and a statute-based example. From history and the common law, *Spokeo* noted that common law defamation cases have long allowed plaintiffs to sue even though their actual damages are difficult to prove. *Id.* From Congress, *Spokeo* cited two information-rights cases, *Federal Election Comm'n v. Akins*, 524 U.S. 11, 20-25 (1998), and *Pub. Citizen v. U.S. Dep't of Justice*, 491 U.S. 440, 449 (1989), both of which involved plaintiffs who sought information that Congress had decided to make available to the public. *Spokeo*, 136 S. Ct. at 1549-50. There was no particular *substantive* standard of conduct set by the pertinent provisions of the information-access statutes involved in those cases. Indeed, *Public*

[9]This Opinion uses (cleaned up) to indicate that internal quotation marks, alterations, and citations have been omitted from quotations. *See* Jack Metzler, *Cleaning Up Quotations*, 18 Journal of Appellate Practice and Process 143 (2017).

Citizen cited to prior cases involving the Freedom of Information Act, and declared, "Our decisions interpreting the Freedom of Information Act have never suggested that those requesting information under it need show more than that they sought and were denied specific agency records." *Pub. Citizen*, 491 U.S. at 449 (citing cases). These *procedural*-rights-only cases led *Spokeo* to explain that "the violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact. In other words, a plaintiff in such a case need not allege any *additional* harm beyond the one Congress identified." 136 S. Ct. at 1549 (emphasis in original).

Applying these principles to this case, with the aid of more recent Seventh Circuit cases, it is clear that Google's retention of Plaintiffs' unique face templates did not cause them a concrete injury for Article III standing purposes. The more difficult question is whether the creation of the face templates constitutes an injury-in-fact on its own. But that too falls short of satisfying Article III's concreteness requirement.

B. Retention of Face Scans

First up is Plaintiffs' claim that Google retained or stored their face templates in violation of the Act.[10] The Act requires that any private entity in possession of biometric information or identifiers must develop and make available to the public a retention schedule and guidelines for destroying that information, 740 ILCS 14/15(a),

[10]As noted earlier, for the purposes of deciding this motion, the Court assumes that the face templates are "biometric identifiers" under the Act, 740 ILCS 14/10, and that Google did not provide disclosures or obtain the consent as required by the Act, *id.* § 14/15.

and provides certain standards for storing, transmitting, and protecting the information, *id.* § 14/15(e). By not providing the required disclosure or obtaining the required consent, Plaintiffs argue that Google violated their right to control their own biometric identifiers and information, which Plaintiffs assert is a right of privacy. Pls.' Resp. Br. at 3-4 (citing Pls. Statement Add. Facts ¶ 3 (quoting Weiss Dep. Tr. at 176:21-177:2 ("I believe that my biometric information or identifier is very sensitive. I think it's akin to my DNA, to a fingerprint. To have that stored, collected, is, again, that in and of itself, when done so against my consent or without my consent, it's a damage, I think.")); Pls. Statement Add. Facts ¶ 4 (citing Rivera Dep Tr. at 78:10-14)); R. 166-2, Exh. B, Rivera Dep Tr. at 59:15-19 ("Google is putting me at risk for potential hackers. … I feel like it's putting me—pretty much my identity in danger."); *id.* at 61:8-9 ("I feel like my identity was harmed so that is my property.").

The Seventh Circuit has definitively held that retention of an individual's private information, on its own, is not a concrete injury sufficient to satisfy Article III. *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 912-13 (7th Cir. 2016). In *Gubala*, a cable subscriber alleged that Time Warner Cable had unlawfully retained information that he had provided—including his date of birth, address, phone number, and social security number—in violation of the Cable Communications Policy Act. *Id.* at 910. The Seventh Circuit acknowledged that there would be "a *risk* of harm" if Time Warner had "given away or leaked or lost any of his personal information or ... ha[d] the information stolen from it." *Id.* (emphasis in original). But there were no facts suggesting that the information had been further disclosed or that

there truly was a risk of disclosure. *Id.* at 910-11. So even though the statute was violated, *Gubala* held that mere retention of an individual's personal data (without disclosure or risk of disclosure) was insufficient to confer Article III standing. *Id.* at 912-13. Yes, the subscriber did "*feel* aggrieved," but that by itself did not cause him a concrete injury. *Id.* at 911 (emphasis in original); *see also Groshek v. Time Warner Cable, Inc.*, 865 F.3d 884, 886-87, 889 (7th Cir. 2017) (plaintiff lacked standing to sue for a violation of the Fair Credit Reporting Act where the defendant obtained a credit report without providing the required disclosures; although the defendant's action violated plaintiff's privacy, it was merely a "statutory violation completely removed from any concrete harm or appreciable risk of harm").

Setting aside *how* Google obtained Plaintiffs' face templates (which will be addressed in the following section), Plaintiffs have not offered evidence about the retention of their face templates that overcomes the obstacle in *Gubala.* Plaintiffs do not dispute that: their face templates have not been shared with other Google Photos users or with anyone outside of Google itself; there has not been any unauthorized access to the accounts or data associated with their face templates or face groups; and hackers have not obtained their data. Pls. Resp. Def. SOF ¶¶ 49-52. In other words, all that Plaintiffs can point to on the issue of retention is a privacy concern that *Gubala* holds is insufficient to satisfy Article III's concrete-injury requirement.

To demonstrate a heightened risk of harm, Plaintiffs filed a notice of supplemental information, with an accompanying news article and a Google blog entry, reporting that a software bug gave outside developers access to the data of

around 500,000 Google+ users between 2015 and March 2018. R. 203, Exh. A, 10/08/18 WSJ Article; *id.*, Exh. B, 10/08/18 Project Strobe Blog. Google+ is another Google product, distinct from Google Photos. According to Plaintiffs, the exhibits show that Google decided not to disclose the issue to avoid regulatory scrutiny and reputational damage. *Id.* More recently, Plaintiffs filed another notice, which reports yet another software bug that compromised the private information of around 52½ million Google+ users, which Google again kept quiet for about a week before disclosing. R. 204, Exh. A, 12/10/18 The Keyword Blog. Even assuming, as is appropriate at summary judgment, that these breaches happened and that Google failed to disclose them fast enough, these disclosures have little bearing on the facts of *this* case. None of the disclosures pertain to the accounts of Google Photos users, nor is there any evidence of a connection between the disclosures of Google+ account data to Google Photos accounts or data. *Id.* So this newly presented information does not create a genuine dispute undermining Google's argument that "[t]here is no evidence of any unauthorized access to the *Google Photos accounts* and related data of Weiss and Gutierrez," Def. SOF ¶ 50 (emphasis added), nor is there "evidence that the face templates, face groups, or face labels from the photographs of Weiss and Rivera in Weiss and Gutierrez's *Google Photos accounts*, respectively, have been shared outside of Google." *Id.* ¶ 52 (emphasis added).[11]

[11]Although neither party discusses Google Photo Application Programming Interfaces (APIs), it appears that there are APIs for Google Photos. *See* R. 166-2, Maya Decl., Exh. H (email from Google employee thanking a person from "PM Mobile Vision APIs/Platform" for help with improving FaceNet technology); *see also* https://developers.google.com/photos/ (website for Google Photos APIs). "Google makes user data available to outside developers through more than 130 different public channels known as application programming

When a plaintiff relies on a risk of future harm to satisfy Article III's injury requirement, the plaintiff must establish, at the very least, a "substantial risk" that the future harm will occur. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013). The circumstances underlying the Google+ data breach do not come close to the kinds of situations in which the risk of future harm satisfies Article III concreteness requirements. *Compare Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968-69 (7th Cir. 2016) (hackers already had breached the defendant's database and stolen customers' payment-card information, so the risk of identity theft and the precautions customers took to mitigate the risk constituted a concrete injury) and *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (same), *with In re VTech Data Breach Litig.*, 2017 WL 2880102, at *4-5 (N.D. Ill. July 5, 2017) (a hacker accessed and copied plaintiffs' data—including names, addresses, and birthdates—from defendant's online communication platform connected to a children's game, but because plaintiffs did not plausibly allege that the disclosure of that data increased their risk of identity theft or fraudulent transactions, they lacked standing). It is true that the Illinois legislature has concluded that identity theft of

---

interfaces, or APIs." 10/08/18 WSJ Article at 2. But the mere existence of APIs does not mean that, without a bug, Google was sharing photos or face templates with outside parties, since APIs "usually require a user's permission to access any information … ." *Id.* So Plaintiffs could not rely on the mere existence of Google Photo APIs to confer standing (nor have they done so in any filing).

The Google+ bugs affected Google+ APIs, so ostensibly a bug causing a data breach *could* also affect a Google Photos API. But as noted above, there is no evidence that any such bug has affected Google Photos or any Google Photos APIs, so any such harm is purely speculative. That said, if Google is aware of any bug or data breach to any Google Photos API or Google Photos itself, it should have already reported them to Plaintiffs (as supplemental discovery) and to the Court (in a supplemental filing), and must do so immediately if a Google Photos breach occurred.

biometric information poses an additional harm beyond theft of other personal identifiers: it is not as easy to change biometric information as it is to get a new social security number or a new credit card number, *see* 740 ILCS 14/5(c) ("Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information … once compromised, the individual has no recourse … ."). But Plaintiffs here have not offered enough evidence, even when viewed in their favor, demonstrating a substantial risk that their own information will be disseminated to anyone outside of Google. The Google+ data breach does not support Article III standing.

With regard to the retention violation, all Plaintiffs are left with is their testimony that they felt their privacy rights were violated, but "*feel*[*ing*] aggrieved," without more, does not establish a concrete injury. *Gubala*, 846 F.3d at 911, 913. Plaintiffs' retention claims must be dismissed for lack of Article III standing.

C. Collection of Face Scans

The much closer question on standing is whether Plaintiffs suffered a concrete injury arising from Google's creation of their face templates without their knowledge.[12] Viewing the facts in the light most favorable to Plaintiffs, they did not know Google created their face templates based on the photos of Plaintiffs' faces uploaded to Google Photos. *See* Pls. Resp. Def. SOF ¶ 29 (quoting Weiss Dep. Tr. at 171:21 ("I would not have consented if I had known that biometric information was

[12]To be crystal clear, the Court reiterates that it is assuming for purposes of this Opinion that Plaintiffs' face templates are biometric identifiers or information as defined by the Act, 740 ILCS 14/10, and that Google did not provide the required disclosures or obtain the required consent, *id.* § 14/15.

being gathered, collected, stored.")); Pls. Statement of Add. Facts ¶ 2 (quoting Rivera Dep. Tr. at 9:9-13 "[Ms. Gutierrez] stated that if I was aware that Google had this face recognition where they were using biometric information, which is a template of my face, so whenever my phot[o]s were taken with her device, they were automatically uploaded. I was then upset, very angry at the fact that they were taken without my consent and I didn't have any control as to whether or not they were able to be used.")).

Gubala does not directly answer this issue because here Plaintiffs did not know that their face templates were being created by Google. Google argues otherwise, contending that "[i]t makes no difference that *Gubala* referred to 'retention' of data, while Google here is alleged to have impermissibly obtained and retained the face templates." Def.'s Br. at 11. But *Gubala* did not merely "refer" to retention of private information—instead, retention was the limit of the holding, because the cable subscriber *knew* that Time Warner had his information. In fact, the subscriber himself provided the information when signing up for cable service. 846 F.3d at 910. The same fact—that the plaintiffs knew or should have known that their biometric information was being collected by the defendant—also distinguishes other district court cases relied on by Google. *See, e.g.*, *Howe v. Speedway LLC*, 2018 WL 2445541, at *6 (N.D. Ill. May 31, 2018) (plaintiff's "fingerprints were collected in circumstances under which any reasonable person should have known that his biometric data was being collected."); *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 515 (S.D.N.Y. 2017), *aff'd in relevant part, vacated in part, remanded sub*

nom. Santana v. Take-Two Interactive Software, Inc., 717 F. App'x 12 (2d Cir. 2017) ("The allegations show that the plaintiffs, at the very least, understood that Take-Two had to collect data based upon their faces in order to create the personalized basketball avatars, and that a derivative of the data would be stored in the resulting digital faces of those avatars so long as those avatars existed."). Here, Plaintiffs did not knowingly place their finger on a fingerprint scanner (as in *Howe*) or stare up-close at a camera for about 15 minutes while a camera scanned their face and heads (as in *Vigil*, 235 F. Supp. 3d at 505). Instead, they merely took pictures of themselves (or allowed them to be taken), which then were automatically uploaded to Google Photos where their face template was created. So *Gubala*, *Howe*, and *Vigil* are not directly on point when evaluating the extent of the privacy intrusion of Google Photos.

On the flip side, however, recent cases that have found Article III standing where the plaintiff *did not know* of the collection of biometric information are themselves also not directly on point, because in those cases the information was then disclosed to a third-party. In two recent cases, plaintiffs have successfully shown injury-in-fact because the defendant disclosed a fingerprint scan to a third-party without informing the plaintiff or obtaining the plaintiff's consent. *See Miller v. Sw. Airlines Co.*, 2018 WL 4030590, at *3 (N.D. Ill. Aug. 23, 2018); *Dixon v. Washington & Jane Smith Cmty.-Beverly*, 2018 WL 2445292, at *10 (N.D. Ill. May 31, 2018). Although the opinions included dicta suggesting that collection of biometric data without the plaintiff's knowledge can constitute a concrete risk of harm, ultimately the courts relied on both the absence of consent in collection of the fingerprint *and*

the later disclosure of the fingerprint without consent *Miller*, 2018 WL 4030590, at *3 ("A violation of [the Act's] notice and consent provisions does not create a concrete risk of harm to a plaintiff's right of privacy in his or her biometric data unless the information is collected or *disseminated without the plaintiff's knowledge or consent*.") (emphasis added); *Dixon*, 2018 WL 2445292, at *9 ("Obtaining or *disclosing* a person's biometric identifiers or information *without her consent or knowledge* necessarily violates that person's right to privacy in her biometric information.") (emphasis added). As discussed earlier, Plaintiffs concede that their face templates have not been shared—and there is no showing that there is an imminent risk that they will be shared—with anyone outside of Google. Pls. Resp. Def. SOF ¶¶ 47, 49-52. So the two district-court decisions are not directly applicable to this case.

As the parties discuss in detail, the most factually analogous case is *Patel v. Facebook Inc.*, 290 F. Supp. 3d 948 (N.D. Cal. 2018).[13] In *Patel*, the plaintiffs alleged that Facebook applies facial-recognition software to pictures uploaded by users, and then creates and stores face templates based on geometric relationships of facial features—all without users' consent. *Id.* at 951. The plaintiffs did not allege any injury (such as emotional distress, physical harm, dissemination to a third-party, or adverse employment impacts) beyond the violation of the Act's notice-and-consent requirements. *Id.* at 951, 954; *see also* Amend. Compl., *In re Facebook Biometric Info. Privacy Lit.*, No. 3:15-cv-03747, R. 40 (N.D. Cal. Aug. 28, 2015). The district court

[13]On May 29, 2018, the Ninth Circuit granted Facebook's petition for interlocutory appeal of the district court's order granting class certification. *Patel v. Facebook, Inc.*, USCA No. 18-15982 (9th Cir. May 30, 2018). No oral argument has been scheduled yet.

denied Facebook's motion to dismiss for lack of standing, holding that the plaintiffs had sufficiently alleged a concrete injury to satisfy Article III based solely on the violation of the Act. *Patel*, 290 F. Supp. at 956.

Patel placed great weight on the legislative findings and intent underlying the Act, and indeed (and as discussed above) *Spokeo* does instruct courts to respect legislative judgments in identifying intangible harms. As recounted by *Patel*, the Illinois legislature found that (1) biometrics are uniquely sensitive and when compromised, put individuals at a heightened risk for identity theft; (2) biometric technology is cutting edge, and "[t]he full ramifications of biometric technology are not fully known"; (3) the public is "weary"[14] of using biometrics when tied to personal information; and (4) regulating biometric collection, use, and storage serves the public interest. *Id.* at 953 (citing 740 ILCS 14/5(b)-(e), (g)). The district court reasoned that these legislative findings, combined with the notice-and-consent requirements (among other requirements of the Act), left "little question that the Illinois legislature codified a right to privacy in personal biometric information" and that the legislature determined "that a violation of [the Act's] procedures would cause actual and concrete harm." *Id.*

Because a statutory violation is not *necessarily* enough for Article III standing, it is important to discern exactly on what grounds *Patel* relied for finding concrete harm. *Patel* appears to rely on two specific points: first, as the Illinois legislature found, biometric information "cannot be changed if compromised or misused." *Id.* at

[14] It is possible that the word "weary" in the Act, 740 ILCS 14/5(d), was intended to be "wary."

954. So when there is a violation of the Act, *Patel* asserted, "the right of the individual to maintain her biometric privacy vanishes into thin air." *Id.* Second, later in the opinion, *Patel* distinguished two cases that had rejected standing under the Act. In those two cases, the plaintiffs knew that their biometric information was being collected by the defendants. *Id.* at 955 (discussing *Vigil*, 235 F. Supp. 3d at 513 (scans of plaintiffs' faces that took 15 minutes and required plaintiffs to consent by pressing "continue" after reading a notice stating a "face scan" might be recorded); and *McCullough v. Smarte Carte, Inc.*, 2016 WL 4077108 (N.D. Ill. Aug 1, 2016) (plaintiffs scanned their fingerprints to rent a locker)). *Patel* explained that the injuries there were not sufficiently concrete because the plaintiffs "indisputably knew that their biometric data would be collected before they accepted the services offered by the businesses involved." *Patel*, 290 F. Supp. 3d at 955. So *Patel*'s holding stands on two pillars: the risk of identity theft arising from the permanency of biometric information, as described by the Illinois legislature, and the absence of in-advance consent to Facebook's collection of the information. *Id.*

This is a close question, but even when drawing all inferences in Plaintiffs' favor, neither pillar supports a finding of concrete injury. First, as discussed in detail earlier, there is no evidence of a substantial risk that the face templates will result in identity theft. It is true that if an unintended disclosure happens, then there are few ways to change biometric information, and federal courts should follow the legislature's lead in considering that immutability in deciding what is a "substantial" risk. But even taking that permanency into account does not justify an across-the-

board conclusion that *all* cases involving *any* private entity that collects or retains individuals' biometric data present a sufficient risk of disclosure that concrete injury has been satisfied in *every* case.

On the second pillar of *Patel*, there is no legislative finding that explains why the absence of consent gives rise to an injury that is *independent* of the risk of identity theft. *See* 740 ILCS 14/5(a)-(g). Indeed, the only specific injury described by the Act's findings is the risk of identity theft, 740 ILCS 14/5(c), (d). The other findings only set forth broad conclusions, like the "public welfare, security, and safety will be served" and the "full ramifications of biometric technology are not fully known." 740 ILCS 14/5(f), (g). The generality of the legislature's findings is especially damning when considering whether unconsented face scans are sufficiently concrete for Article III purposes. Most people expose their faces to the general public every day, so one's face is even more widely public than non-biometric information like a social security number. Indeed, we expose our faces to the public such that no additional intrusion into our privacy is required to obtain a likeness of it, unlike the physical placement of a finger on a scanner or other object, or the exposure of a sub-surface part of the body like a retina. There is nothing in the Act's legislative findings that would explain why the injury suffered by Plaintiffs here—the unconsented creation of face templates—is concrete enough for Article III purposes. As important and instructive as legislative judgments are in evaluating intangible harms, the Act does not support a finding that the concrete-injury requirement has been met in this case.[15]

[15]This holding is limited to the specific circumstances of this case, which challenges face scans. Likewise, this holding of course does not preclude the legislature from making

Moving on from legislative findings, *Spokeo* instructs courts to also examine possible analogues to common law harms that historically have supported a finding of Article III injury-in-fact. *Spokeo*, 136 S. Ct. at 1549 ("[I]t is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.") In this case, Plaintiffs' response brief outlines the historical development of the right to privacy in American law, which was "fueled by social and technological change." Pls.' Resp. Br. at 8. They argue that the Act directly follows from common law privacy torts. *Id.* at 8-9. It is true that the alleged injury in this case need not square on all fours with a common law privacy tort. Plaintiffs are correct that they do not have to adequately state a claim under a common law tort; otherwise, they would just pursue a common law claim, and *Spokeo* must have meant more than that when it authorized claims for harms that bear a close relationship to common law claims. Pls.' Resp. Br. at 10; *see also Whitaker v. Appriss, Inc.*, 229 F. Supp. 3d 809, 813 (N.D. Ind. 2017) (noting that the "close relationship" test does not require "sameness"). At the same time, however, the common law tort must bear a close relationship to the alleged injury in *this* case in order for the common law analogue to be instructive. *See Spokeo*, 136 S. Ct. at 1549; *see also Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017) (statutory violation led to "unsolicited

---

additional findings either now or in the future. It is not hard to imagine more concrete concerns arising from facial-recognition technology, especially as it becomes more accurate and more widespread (along with video-surveillance cameras) to the point that private entities are able to use the technology to pinpoint where people have been over extended time periods.

contact" and "disturb[ing of] solitude," similar to nuisance tort); *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1114-15 (9th Cir. 2017) (statutory violation resulted in "dissemination of false information," similar to defamation tort).

To start, there are four well-established common law privacy torts: (a) unreasonable intrusion upon someone's seclusion; (b) appropriation of a person's name or likeness; (c) unreasonable disclosure of private facts; and (d) publicity that unreasonably places the other in a false light. Restatement (Second) of Torts § 652A (1977). Plaintiffs rightly do not argue that Google's alleged conduct is anything like the public disclosure of private facts or false-light invasion of privacy. Pls.' Resp. Br. at 8-10. That leaves intrusion on seclusion and appropriation of likeness.

Starting with intrusion on seclusion, the Second Restatement of Torts defines this tort as a claim against someone "who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns … if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B (1977). The elements of the tort are "(1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion that is highly offensive or objectionable to a reasonable person; (3) that the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering." *Jacobson v. CBS Broad., Inc.*, 19 N.E.3d 1165, 1180 (Ill. App. Ct. 2014). The third element, that the intrusion be upon a *private* matter, is a necessary predicate for the other elements. *Id.* at 1181; *see also Lovgren v. Citizens First Nat. Bank of Princeton*, 534 N.E.2d 987, 989 (Ill. 1989) ("[T]he core of this tort is the

offensive prying into the *private* domain of another.") (emphasis added). It is this element where the relationship between Plaintiffs' alleged injury and this common law tort breaks down.

First, Plaintiffs cannot show—and do not argue—that Google "intruded into a private place" by receiving photographs of Plaintiffs voluntarily uploaded (by Weiss or Gutierrez) to Google Photos. *See* Pls.' Resp. Br. at 8-11; R. 60, Opinion 2/27/17 at 26 n.11 ("Neither side is arguing that for the purposes of the Privacy Act, Google needed consent to upload the photographs to the cloud."). Second, although Plaintiffs argue that their faces are not public, Pls.' Resp. Def.'s SOF ¶ 60 (disputing "that their faces are public, not private."), Plaintiffs' only evidence to support that assertion is deposition testimony in which they say that their facial *biometrics* are private information. *Id.* (quoting Weis Dep. Tr. at 183:18-19 ("Looking [at someone's face with your eyes] and recording [someone's face with biometric identifiers] are different, as far as I understand."); quoting Rivera Dep. Tr. at 45:15-19 ("[W]hen it's taking my biometric information, that's sensitive information to me. That's my personal information.")). Plaintiffs do not offer evidence to dispute that their *faces* are public—just that their facial *biometrics* are. This is consistent with Fourth Amendment case law that rejects an expectation of privacy in a person's face. *See United States v. Dionisio*, 410 U.S. 1, 14 (1973) (explaining that "[n]o person … can reasonably expect that his face will be a mystery to the world," and holding that an individual's face, when knowingly exposed—even in his own home or office—is not protected by the Fourth Amendment) (citing *Katz v. United States*, 389 U.S. 347, 351 (1967)). Indeed,

Illinois courts have dismissed many intrusion-upon-seclusion claims that were premised on photographs or videos for failure to satisfy the privacy element of the tort. *See Jacobson*, 19 N.E. at 1181 (affirming dismissal where plaintiff was filmed on "readily visible property" and the images of her revealed nothing that was "especially private"); *Schiller v. Mitchell*, 828 N.E.2d 323, 326, 329 (Ill. App. Ct. 2005) (defendants did not intrude upon plaintiffs' seclusion by capturing surveillance video of plaintiffs on their property, including within their garage, because passersby could see the same things from different angles); *see also* Restatement (Second) of Torts § 652B cmt. c (there is no intrusion-upon-seclusion liability for "observing [a plaintiff] or even taking his photograph while he is walking on the public highway, since he is not then in seclusion, and his appearance is public and open to the public eye"). It bears repeating that Plaintiffs need not satisfy the elements of a common law tort to show Article III injury. But there is a wide gap between the alleged injury here—the creation and retention of the face templates—and the privacy interest protected by the intrusion-on-seclusion tort. All that Google did was to create a face template based on otherwise public information—Plaintiffs' faces. *See Patel v. Zillow, Inc.*, 2017 WL 3620812, at *10 (N.D. Ill. Aug. 23, 2017) (defendant did not intrude into private matters when it created real-estate data derived from public information).

Another element of the intrusion-on-seclusion tort shows the disconnect between the common law claim and this case: the creation of face templates is not a "highly offensive" intrusion.[16] As discussed earlier, the templates are based on

[16]Plaintiffs argue that whether the creation of face templates was "highly offensive" would "clearly be for a jury to decide at trial, not for the Court to decide at summary

something that is visible to the ordinary eye, that is, Plaintiffs' faces. And the crux of the tort is the intrusion itself, not what is done with the fruits of the intrusion (if there are any fruits) later. In other words, "[t]he basis of the tort is *not* publication or publicity." *Lovgren*, 534 N.E.2d at 989 (emphasis added). So what Google did with the photographs of Plaintiffs' faces—that is, using them to create face templates—is irrelevant when comparing this case to an intrusion-on-seclusion claim. In any event, the record shows that Google only used the facial images to create face templates that organize Plaintiffs' photographs in private Google Photos accounts. Plaintiffs do not present any evidence showing that Google commercially "exploited" their faces or the face templates they created. Without more, Plaintiffs' injury in this case does not bear a close relationship to the tort of intrusion upon seclusion.[17]

That leaves the tort of appropriation of likeness. This common law tort protects an individual's "interest … in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or others." Restatement (Second) of Torts § 652C cmt. a (1977).[18] This interest is

---

judgment." Pls.' Resp. Br. at 10. If Plaintiffs asserted the intrusion-on-seclusion claim, then that argument would have greater force, because the merits of the claim could be a question for the jury. But the analysis at hand is whether Plaintiffs have sufficiently established an injury-in-fact under Article III for purposes of subject matter jurisdiction. There is no general Seventh Amendment jury trial right for issues of subject matter jurisdiction, and Plaintiffs offer no precedent that the close-relationship analysis, as explained in *Spokeo*, is a matter for the jury to decide.

[17]Plaintiffs' argument that the creation of face templates is similar to "restaurants [] dust[ing] their customers' glasses for fingerprints and stockpil[ing] those identifiers," Pls.' Resp. Br. at 10, is misplaced. Fingerprints are not held out to the public like faces, which are visible to the ordinary eye. Applying a template to a face on a voluntarily uploaded photograph is very different from collecting the tiny physical remnants left by ridges on a person's fingers.

[18]In Illinois, the common law tort of appropriation of likeness was replaced with the Right of Publicity Act, 765 ILCS 1075/30, effective in 1999. *Trannel v. Prairie Ridge Media,*

invaded when a defendant uses the likeness "to advertise [its] business or product," "for some similar commercial purpose," or "for [its] own purposes and benefit." *Id.* cmt. b. Plaintiffs have not shown that Google has done anything closely related to appropriation of their likenesses. In their Rule 56.1 Statement, Plaintiffs dispute that "[t]here is no evidence that any of the data generated by Google Photos was used in any way except to help organize the photographs in Wiess's and Gutierrez's accounts." Pls. Resp. Def. SOF ¶ 59; *see also* Pls. Statement Add. Facts ¶ 6. But the evidence offered in their response fails to adequately support their denial. Plaintiffs cite to an article that describes ways in which Google's facial recognition technology *could* be used in the future, including data mining, targeted advertisements, and filtering content, Pls. Statement Add. Facts ¶ 6 (citing Maya Decl., Exh. K), as well as an email chain among Google employees forwarding an article discussing similar "likely" uses, *id.* (citing Maya Decl., Exh. I). These exhibits only demonstrate *future* potential uses of Google's facial recognition technology; they do not suggest that Google currently employs these practices, that Google likely will do so in the future without consent, or that Google used Plaintiffs' data in this way. So the evidence falls well short of a substantial likelihood that Plaintiff's will suffer any of those injuries. The only other tack that Plaintiffs could possibly take is to argue that Google "mapped Plaintiffs' faces, creating, collecting, storing, and exploiting their unique biometric identifiers for its own competitive advantage in the marketplace for photo-sharing services." Pls.'

Inc., 987 N.E.2d 923, 929 (Ill. App. Ct. 2013). The Act has nearly identical elements to the common law tort, and a plaintiff must allege three elements: "(1) an appropriation of one's name or likeness; (2) without one's consent; and (3) for another's commercial benefit." *Id.*

Resp. Br. at 2. But Plaintiffs do not develop this argument or offer evidence in support of it. Google's use of the face templates for the sole purpose of organizing photographs does not bear a "close relationship" to harms caused by appropriation of likeness.

With neither a legislative judgment nor a common law analogue (or anything else) to support a finding of concrete injury, the Court concludes that Plaintiffs have not demonstrated an injury-in-fact sufficient to confer Article III standing.[19] This case presented close legal questions, which is not uncommon when it comes to technological advances,[20] and the Court appreciates the able presentations of both sides.

IV. Conclusion

Google's motion for summary judgment is granted. The Court lacks subject matter jurisdiction because Plaintiffs have not suffered concrete injuries for Article III purposes. In light of that holding, there is no need to opine on the statutory-interpretation arguments (and, in any event, the Illinois Supreme Court has the issue

[19]A court within this District held the plaintiff had alleged an injury-in-fact where the defendant allegedly collected his face scans without his knowledge in violation of the Act. *Monroy v. Shutterfly*, 2017 WL 4099846, *8 n.5 (N.D. Ill. Sept. 15, 2017). But *Monroy* relies on a generally described privacy invasion, rather than engage in an analysis of specific common law torts (it also does not appear that the parties precisely teed up this issue for the district court in that case, as the defendant did not challenge the plaintiff's standing). *Id.*

[20]The difficulty in predicting technological advances and their legal effects is one reason why legislative pronouncements with minimum statutory damages and fee-shifting might reasonably be considered a too-blunt instrument for dealing with technology. Of course, there might be policy considerations that weigh in favor of taking the broader approach.

under advisement). The case is dismissed for lack of subject matter jurisdiction and the status hearing of January 22, 2019 is vacated.

ENTERED:

s/Edmond E. Chang
Honorable Edmond E. Chang
United States District Judge

DATE: December 29, 2018