BIOMETRIC PRIVACY LITIGATION: IS UNIQUE PERSONALLY IDENTIFYING INFORMATION OBTAINED FROM A PHOTOGRAPH BIOMETRIC INFORMATION?

By Natasha Kohne and Kamran Salour[1]

I. FACIAL RECOGNITION TECHNOLOGY: THE ABILITY TO PERSONALLY IDENTIFY SOMEONE FROM A PHOTOGRAPH

A. Social Media Sites Store Millions of Individualized Faceprints Generated From Photographs

Millions of people upload their photographs to social media sites such as Google and Facebook every day.[2] Google Photos touts more than 200 million monthly active users.[3] Shutterfly's ThisLife database stores roughly 18 billion images.[4] And Facebook claims that it has already uploaded 250 billion user photos, with 350 million more uploads daily.[5]

But in today's technological world, with only a mathematical algorithm, any person's face from a photograph can be analyzed and converted into an individualized "faceprint"—a unique identifying tag analogous to a fingerprint.[6] Creating a faceprint is surprisingly simple: typically, an algorithm measures the relative position, size, or shape of the eyes, nose, cheekbones, and jaw; these measurements are then compared with an existing database of images to determine a match.

Though simple, these algorithms are remarkably effective. Google's FaceNet algorithm reportedly identifies faces with 99.63 percent accuracy. Facebook's DeepFace operates at a reported 97.25 percent accuracy rate. Both algorithms significantly outperform the FBI's facial recognition program, which reports an 85 percent success rate.[7] To appreciate the effectiveness of these algorithms consider this: if you present

---

1 Natasha Kohne co-heads Akin Gump's cybersecurity, privacy and data protection practice and is licensed to practice in New York. Ms. Kohne is a partner in Akin Gump's San Francisco office (practicing under the supervision of Akin Gump's California partners) and in Abu Dhabi. Kamran Salour is counsel in Akin Gump's Los Angeles office and is a member of the firm's cybersecurity, privacy and data protection practice. The views expressed in this article are those of the authors and do not necessarily represent the views of Akin Gump Strauss Hauer & Feld LLP, its lawyers, or its clients.

2 Ben Sobol, *Facial recognition technology is everywhere. It may not be legal.,* WASH. POST, (June 11, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/.

3 Kia Kokalitcheva, *Google Photos Has Added Millions of New Users,* FORTUNE (May 18, 2016), http://fortune.com/2016/05/18/google-photos-200-million/.

4 Ricardo Bilton, *Shutterfly buys ThisLife in an attempt to create the perfect photo service, VENTURE BEAT (Jan. 7, 2013), http://venturebeat.com/2013/01/07/shutterfly-buys-thislife/.*

5 Jam Kotenko, *Facebook reveals we upload a whopping 350 million photos to the network daily,* DIGITAL TRENDS (Sept. 18, 2013), http://www.digitaltrends.com/social-media/according-to-facebook-there-are-350-million-photos-uploaded-on-the-social-network-daily-and-thats-just-crazy/.

6 Avi Asher-Schapiro, *Facial Recognition Technology Is Big Business—And It's Coming For You,* VICE NEWS (Aug. 13, 2015), https://news.vice.com/article/facial-recognition-technology-is-big-business-and-its-coming-for-you.

7 *Id.*

a person with two pictures, that person can tell at around a 97 percent accuracy rate whether the same person is in each photograph.[8]

As is evident from these comparative statistics, a company can generate readily a faceprint and identify a previously unknown individual from that faceprint with facial recognition technology with astonishing precision.

B. Faceprints Raise Potential Biometric Privacy Issues

Both Google and Facebook have amassed considerable faceprint databases. So far, Google Photos has applied automatically more than 2 trillion identifying tags to photographs in its database.[9] Facebook has not disclosed the size of its faceprint database, but it has called its repository "the biggest dataset in the world."[10]

But facial recognition technology sparks a series of privacy discussion points. First, it raises the topic of consent: "Unlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a [greater] distance, without the knowledge or consent of the person being identified. Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere—on a lamp post, attached to an unmanned aerial vehicle or, now, integrated into the eyewear of a stranger."[11]

Second, facial recognition technology raises the topic of safeguarding. Biometric information is unlike other unique personal information such as social security or credit card numbers that if lost or stolen, can be replaced. Biometric information is biologically unique to an individual; if compromised, such information is irreplaceable. Therefore, it is important to know for what purpose biometric information will be collected, how it will be used, and how (and for how long) it will be stored before being destroyed.

Yet another question surrounding biometrics in the facial recognition context—and this article's primary focus—is does information derived from facial recognition technology constitute biometric information? Principally, must a facial recognition scan take place in-person, or does one capture biometric data by simply scanning a photograph?

As is often the case, technology outpaces the law, so the answer to this question remains unsettled. To compound matters, there is no federal statute that governs biometric privacy. And without a federal statute, states are left to create their own statutes to protect their citizens' biometric information. Only two states, Illinois and Texas, have statutes directed to biometric privacy. Texas' biometric statute, Capture or Use of Biometric Identifier (CUBI)[12], has not been the subject of judicial interpretation, while

---

8 Russell Brandom, *Why Facebook is beating the FBI at facial recognition,* The Verge (July 7, 2014), http://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition.

9 Kokalitcheva, *supra* note 3.

10 Sobol, *supra* note 2.

11 Press Release, Sen. Franken Raises Concerns about Facial Recognition App that Lets Strangers Secretly Identify People (Feb. 5, 2014), https://www.franken.senate.gov/?p=press_release&id=2699.

12 Tex. Bus. & Com. Code Ann. § 503.001 (2009).

judicial interpretation of Illinois' biometric statute, Biometric Information Privacy Act (BIPA)[13] has yielded results that are seemingly at odds with BIPA's plain text.

***

Part One of this Article discusses BIPA's origins, the obligations BIPA imposes on individuals and companies, and key BIPA-defined terms. **Part Two** analyzes how federal courts have interpreted BIPA's scope; specifically, whether under BIPA information derived from photographs constitutes biometric information. **Part Three** identifies common jurisdictional and constitutional defenses to BIPA claims and discusses their relative success. **Part Four** explores proposed amendments to BIPA and whether existing and proposed biometric statutes in other states consider unique identifying information derived from photographs to be biometric information. **Part Five** concludes with a discussion on how the existing uncertain biometric legal landscape has taken the focus off of protecting biometric information and instead given savvy plaintiffs' lawyers license to assert multi-million dollar class action suits against companies alleging BIPA violations but devoid of allegations that an individual's biometric information has been compromised.

II. PART ONE: THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT (BIPA)

A. BIPA Was Enacted to Safeguard the Biometric and Corresponding Financial Data of Illinois Residents

In 2008, the Illinois legislature faced a dilemma: Pay By Touch, a California-based company that allowed people to pay for goods and services with only a swipe of a finger,[14] was in bankruptcy, and the California bankruptcy court had just approved the sale of Pay By Touch's database.[15] This was no ordinary database, however. This database housed the fingerprint and financial data of all of Pay By Touch's former customers. Importantly for the Illinois legislature, this database included the fingerprint and corresponding financial data of thousands of Illinois citizens; Illinois had served as a pilot testing site for new applications of biometric-facilitated financial transactions, including Pay By Touch's finger-scan technology. Pay By Touch's bankruptcy posed a serious risk to Illinois citizens whom were left wondering what would happen to their fingerprint and financial data stored in Pay By Touch's database.

Illinois recognized that its citizens needed their biometric information protected.[16] "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once

---

13 740 Ill. Comp. Stat. § 14/1, et seq. (2008).

14 Shubha, *Failure Story: What Happened to Pay By Touch?,* Let's Talk Payments (Apr. 20, 2015), https://letstalkpayments.com/failure-story-what-happened-to-pay-by-touch/.

15 *Pay By Touch Fades into History As Lenders Buy Core Assets,* Digital Transactions (Apr. 7, 2008), http://www.digitaltransactions.net/news/story/Pay-By-Touch-Fades-into-History-As-Lenders-Buy-Core-Assets.

16 *See* IL H.R. Tran. 2008 Reg. Sess. No. 276, at 249 (May 30, 2008) (Statement of Rep. Kathleen A. Ryg).

compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[17]

The Illinois Legislature responded by enacting BIPA,[18] the first state statute focused on the regulation of biometric information in consumer financial transactions. Put broadly, BIPA aims to set "collection and retention standards while prohibiting the sale of biometric information."[19]

From its 2008 enactment until 2015, BIPA remained largely unnoticed, if not altogether unknown. Then, in 2015, three Illinois residents sued Facebook alleging that Facebook's "Tag Suggestions" feature collects, stores, and uses biometric information (*i.e.*, faceprints) in violation of BIPA.[20] Though seemingly divorced from the discrete intent of BIPA to secure biometric information used in financial transactions,[21] this suit sparked several more putative class actions against various social media companies' alleged use of photographic-based facial recognition technology.

B. An Individual's or Company's Obligations under BIPA

BIPA proclaims that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[22]

To achieve this purpose, BIPA makes it unlawful for a ***private entity*** to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's ***biometric identifiers*** or ***biometric information***, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."[23]

If a private entity fails to comply with these requirements, it is subject to civil suit and, at minimum, statutory penalties, ***per each violation***. In particular, BIPA authorizes any person aggrieved by a BIPA violation to file suit against an offending party, and the prevailing party may recover, among other things, $1,000 for each negligent violation, $5,000 for each intentional violation, and reasonable attorneys' fees.[24]

---

17 740 Ill. Comp. Stat. § 14/1, et seq. (2008).

18 *Id.*

19 *See IL H.R. Tran. 2008 Reg. Sess. No. 276, at 249.*

20 *In re Facebook Biometric Information Privacy Litigation,* No. 15-cv-03747-JD, ___ F. Supp. 3d ___, 2016 WL 2593853, at *1 (N.D. Cal. May 5, 2016).

21 Stephanie N. Grimoldby, *Ill. facial recognition law leads to wave of class actions against Facebook, others,* Legal NewsLine (July 6, 2016), http://legalnewsline.com/stories/510954980-ill-facial-recognition-law-leads-to-wave-of-class-actions-against-facebook-others.

22 740 Ill. Comp. Stat. § 14/5(g) (2008).

23 *Id.* § 14/15(b).

24 *Id.* § 14/20.

In short, under BIPA, a private entity must: (1) inform the subject in writing that it collects or stores the subject's biometric identifiers or biometric information; (2) inform the subject in writing of the specific purpose and duration that the biometric identifiers or biometric information will be used, collected, or stored; and (3) obtain the subject's written consent.[25] A failure to comply could subject a private entity to civil suit seeking thousands in civil penalties for each alleged violation. For companies like Snapchat and Shutterfly, the number of alleged violations easily rises to the millions.

C. BIPA's Defined Terms Appear to Exclude from BIPA's Scope Photographs and Information Derived from Photographs

To understand BIPA's scope, one must understand three central defined terms: (1) private entity; (2) biometric identifiers; and (3) biometric information. BIPA defines each of these terms as follows:

- **Private entity** "means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.[26]

- **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."[27]

- **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*** [*i.e.*, writing sample, written signature, photographs] excluded under the definition of biometric identifiers."[28]

---

25 Among its other requirements, BIPA demands a publicly available retention and destruction schedule that establishes a retention schedule and guideline for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. *See id.* § 14/10.

26 *Id.*

27 *Id.* (emphasis added).

28 *Id.* (emphasis added).

Defined Term Under BIPA	Includes	Excludes
Private Entity	Individuals and Companies	Illinois Government Agency
Biometric Identifier	Retina/iris scan; voiceprint; fingerprint; scan of hand or face geometry	Photographs
Biometric Information	Any information based on an individual's biometric identifier used to identify an individual	Information derived from photographs

BIPA's plain text, it would seem, excludes from BIPA's purview ***photographs*** *and any information an individual or company about an individual* ***derived from a photograph.*** *Not everything is as it seems, however.*

III. PART TWO: WHETHER A PLAINTIFF CAN STATE A CAUSE OF ACTION UNDER BIPA WHEN THE ALLEGED BIOMETRIC INFORMATION AT ISSUE WAS DERIVED SOLELY FROM A PHOTOGRAPH

Suits alleging a company's facial recognition technology violates BIPA follow a similar and predictive pattern, the defendant company: (1) allegedly conducted a scan of a photograph of the plaintiff's face; (2) extracted from that photograph the plaintiff's unique geometric data; (3) used that extracted data to create a faceprint of the plaintiff; and (4) compared that faceprint with an existing faceprint database to identify the plaintiff—all without the plaintiff's knowledge or consent.

Two district courts have held that a plaintiff can state a cause of action under BIPA even though the purported biometric information was derived solely from a photograph.[29]

29 *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015); *In re Facebook Biometric Information Privacy Litigation*, No. 15-cv-03747-JD, ___ F. Supp. 3d ___, 2016 WL 2593853, at *1 (N.D. Cal. May 5, 2016).

A. The *Shutterfly* Suit

On December 29, 2015, the Northern District of Illinois issued what is believed to be the first judicial interpretation of BIPA.[30] In that case, the plaintiff Brian Norberg sued Shutterfly, a photo-service company that allows its users to store and organize their photos. In his suit, Norberg, a non-Shutterfly user, claimed that an unnamed Shutterfly user uploaded Norberg's photo while creating a wedding invitation. Norberg alleged that when a Shutterfly user uploads a photo, Shutterfly then scans that photograph for faces, extracts geometric data relating to the unique points and contours of each extracted face, and then uses that data to create and store a template of each face.[31] Shutterfly, therefore, according to Norberg, collected and stored his face template without his informed written consent, in violation of BIPA.[32]

Shutterfly sought to dismiss the complaint for lack of personal jurisdiction[33] and for failure to state a claim.[34] Relying on BIPA's plain text, Shutterfly argued that Norberg cannot state a cause of action because "BIPA clearly and unequivocally states that photographs—and any information derived from photographs—are not within the scope of the law."[35]

At first glance, the court appeared to agree with Shutterfly's interpretation of BIPA. The court noted that BIPA defines a biometric identifier as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," but excludes "writing samples, signatures, ***photographs***, biological samples, demographic data, tattoos, or physical descriptions."[36] The court noted further that BIPA's definition of biometric information does not include information derived from items excluded from the above definition (*i.e.*, photographs).[37] Nonetheless, the court denied Shutterfly's motion to dismiss and held that Norberg did state a cause of action for BIPA:

> Here, [Norberg] alleges that [Shutterfly is] using his personal face pattern to recognize and identify [him] in photographs posted to [Shutterfly's photo sharing websites]. [Norberg] avers that he is not now nor has he ever been a user of [Shutterfly's photo sharing websites], and that he was not presented with a written biometrics policy nor has he consented to have his biometric identifiers used by [Shutterfly]. As a result, the Court finds that Plaintiff has plausibly stated a claim for relief under the BIPA.[38]

---

30 *Norberg,* 152 F. Supp. 3d at 1103.

31 First Amended Class Action Complaint ¶¶ 26-28, *Norberg v. Shutterfly, Inc.*, No. 1:15-cv-05351 (N.D. Ill. June 23, 2015), ECF No. 6.

32 *Id.* ¶¶ 48-51.

33 *See* Part Three, *infra.*

34 *Norberg,* 152 F. Supp. 3d at 1104.

35 Memorandum in Support of Defendants' Motion to Dismiss, Norberg v. Shutterfly, Inc., No. 1:15-cv-05351 (N.D. Ill. April 12, 2016), ECF No. 26.

36 *Norberg*, 152 F. Supp. 3d at 1106.

37 *Id.*

38 *Id.*

Whether Norberg would have prevailed at trial will remain unknown. Ultimately, the parties entered into a settlement agreement and Norberg dismissed the complaint with prejudice.[39]

B. The *Original Facebook* Suit

On May 5, 2016, the Northern District of California similarly held that the plaintiffs could state a cause of action under BIPA even though the purported biometric information was derived from photographs.[40] In 2015, Adam Pezen, Carlo Licata, and Nimesh Patel each brought separate putative class actions in the Northern District of Illinois against Facebook.[41] Those three suits were subsequently consolidated and transferred to the Northern District of California.[42] The class action plaintiffs alleged that Facebook's Tag Suggestions feature—which allegedly scans photographs uploaded by a Facebook user and then identifies faces appearing in those photographs—violates BIPA because it extracts a Facebook user's facial geometry without that user's knowledge or consent.[43]

Facebook argued that BIPA does not apply to its "Tag Suggestions" feature because BIPA excludes photographs and information derived from photographs, and Facebook's feature derived the purported biometric information at issue exclusively from uploaded photographs.[44]

The court denied Facebook's motion and held that the plaintiffs stated a cause of action under BIPA.[45] BIPA regulates the collection, retention, and disclosure of personal biometric identifiers such as the scan of hand or face geometry. "Plaintiffs allege that Facebook scans user-uploaded photographs to create a 'unique digital representation of the face . . . based on geometric relationship of their facial features.' That allegation falls within the scan of face geometry stated in the statute."[46]

The court addressed Facebook's BIPA interpretation as well. The court opined that Illinois legislature enacted BIPA to address emerging biometric technology, such as Facebook's face recognition software, without including physical identifiers that are more qualitative and non-digital in nature.[47] The court went on to interpret photographs to mean physical photographs only: "'Photographs' is better understood to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet. Consequently, the court will not read the statute to categorically exclude

---

39 Stipulation of Dismissal With Prejudice, *Norberg v. Shutterfly*, Inc., No. 1:15-cv-05351 (N.D. Ill. April 12, 2016), ECF No. 91.

40 *In re Facebook Biometric Information Privacy Litigation,* No. 15-cv-03747-JD, ___ F. Supp. 3d ___, 2016 WL 2593853 (N.D. Cal. May 5, 2016).

41 *Id.* at *1-2.

42 *Id.*

43 *Id.*

44 *Id.* at *11.

45 *Id.*

46 *Id.* at *12.

47 *Id.*

from its scope all data collection processes that use images. And to read that categorical exclusion into the statute would substantially undercut it because the scanning of biometric identifiers is often based on an image or photograph."[48]

To date, two separate district courts that have interpreted BIPA, and each such court has held that a plaintiff can state a cause of action under BIPA even if the alleged biometric information is derived solely from photographs. Neither decision is precedential, however.[49]

C. The *Google* Suit

Despite two federal courts refusing to dismiss a BIPA claim on the basis that the purported biometric information was derived from photographs—and therefore is neither a biometric identifier nor biometric information under BIPA—Google has advanced this same argument in defense of a photo-based facial recognition BIPA class action suit.

Plaintiff Lindabeth Rivera sued Google in the Northern District of Illinois.[50] She alleges that Google Photos violates BIPA. "Specifically, Google has created, collected and stored, in conjunction with its cloud-based 'Google Photos' service, millions of 'face templates' (or 'face prints')—highly detailed geometric maps of the face—from millions of Illinois residents, many thousands of whom are not even enrolled in the Google Photos service. Google creates these templates using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces that appear in photos taken on Google 'Droid' devices and uploaded to the cloud-based Google Photos service. Each face template that Google extracts is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person."[51] Rivera does not have a Google Photos account.[52]

Another individual, Joseph Weiss also sued Google under a virtually identical theory.[53] Unlike Rivera, however, Weiss does have a Google Photos account.[54]

On June 17, 2016, Google filed a single motion to dismiss both the Rivera and Weiss complaints. Google maintains that the putative class action should be dismissed for

---

48 *Id.*

49 *See Klein v. Depuy, Inc.,* 476 F. Supp. 2d 1007, 1023 (N.D. Ind. 2007) ("Although federal courts are bound to state court precedents in interpreting state law, there is no authority that requires a district court that is attempting to predict how the highest state court would rule to follow the decision of federal courts sitting in that state."), *aff'd* 506 F.3d 553 (7th Cir. 2007).

50 *See* First Amended Complaint by Lindabeth Rivera, *Rivera v. Google, Inc.*, No. 1:16-cv-02714 (N.D. Ill. May 27, 2016), ECF No. 40.

51 *See id.* ¶ 5.

52 *See id.* ¶ 7.

53 *See* First Amended Complaint by Joseph Weiss ¶ 5, *Rivera v. Google, Inc.*, No. 1:16-cv-02714 (N.D. Ill. May 27, 2016), ECF No. 41.

54 *See id.* ¶ 27.

failure to state a claim because BIPA expressly precludes from its scope photographs and information derived from photographs.[55]

Google's motion also attacks the prior decisions in *Norberg* and *Facebook*. Google maintains that "[t]he decision in *Norberg* contains hardly any reasoning at all, and does not even attempt to explain how BIPA can be read to cover information derived from photographs." Google argues that "[t]he court in *Facebook,* for its part, adopted an interpretation of 'photographs' that neither party before it had advanced, construing the term to refer only to 'paper prints of photographs, not digitized images.'" Google argues further that this " . . . interpretation of BIPA would lead to absurd results—among them that just *taking* a digital photograph would constitute a 'scan of . . . face geometry,' because such a photograph would no longer fall within the exclusion for 'photographs.'"[56]

Google's motion to dismiss is pending. It remains to be seen whether the *Google* court will follow the prior decisions of the *Norberg* and *Facebook* courts, and whether it will address Google's criticisms of those rulings. The *Google* court's decision could open the floodgates to additional putative class actions alleging BIPA violations based on photographic facial recognition.

IV. PART THREE: COMMON JURISDICTIONAL AND CONSTITUTIONAL DEFENSES TO BIPA CLAIMS

A. Courts Have Reached Different Holdings Whether an Interactive Website Is Sufficient to Establish Personal Jurisdiction

Given the uncertainty as to what constitutes biometric information under BIPA, companies facing suit under BIPA have advanced defenses other than personally identifying information derived from a photograph does not constitute biometric information. These defenses have achieved varied success.

One such defense is a lack of personal jurisdiction. At a basic level, a court can only exercise personal jurisdiction (*i.e.,* jurisdiction over the parties to the suit) if there have been sufficient minimum contacts between the defendant and the forum state.[57] If personal jurisdiction does not exist, a court does not have authority to preside over the suit, and the case is dismissed.

In August 2015, an Illinois resident, William Gullen, sued Facebook "resulting from the illegal actions of Facebook in collecting, storing and using Plaintiff's and other similarly situated individuals' biometric identifiers and biometric information . . . without informed written consent in violation of BIPA."[58] Like the suit against Facebook that preceded it, Gullen claims that Facebook's "Tag Suggestions," relies on proprietary facial recognition technology to scan every user-uploaded photo for faces,

---

55 *See* Memorandum by Google, Inc. in Support of Motion to Dismiss for Failure to State a Claim, *Rivera v. Google, Inc.*, No. 1:16-cv-02714 (N.D. Ill. May 27, 2016), ECF No. 49.

56 *Id.*

57 *International Shoe Co. v. State of Wash., Office of Unemployment Comp. and Placement,* 326 U.S. 310, 316 (1945).

58 Complaint ¶ 1, *Gullen v. Facebook.com, Inc.*, No. 1:15-cv-07681 (N.D. Ill. Aug. 31, 2015), ECF No. 1.

extract geometric data relating to the unique points and contours of each face, and then uses that data to create and store, without consent, a template of each face.[59] Gullen does not and has never had a Facebook account.[60]

Facebook filed a motion to dismiss in November 2015. Facebook's motion to dismiss advanced two reasons for dismissal: (1) The Court lacked personal jurisdiction over Facebook; and (2) Gullen could not state a claim under BIPA since his claim rests entirely upon the collection, storage, and use of biometric information that was derived from *photographs* uploaded to Facebook.[61] Facebook argued that to establish personal jurisdiction, Gullen must establish a sufficient "relationship among the defendant, the forum, and the litigation," but Gullen cannot establish the requisite sufficient relationship as he alleges he does not have a Facebook account and has never interacted with Facebook.[62]

On January 21, 2016, the court dismissed Gullen's claim with prejudice.[63] Gullen based his personal jurisdiction claim on the allegation that Facebook "target[s] its facial recognition technology to millions of users who are residents of Illinois."[64] But the court stated that Facebook does not target exclusively its facial recognition technology on Illinois residents; Gullen's complaint alleges that Facebook uses this technology on every user-uploaded photograph.[65] Therefore, Gullen's personal jurisdiction claim is based on the notion that Facebook operates an interactive website, which is insufficient by itself to establish personal jurisdiction.[66]

Conversely, under nearly identical facts, the *Shutterfly* court held that personal jurisdiction did exist. To establish jurisdiction, Norberg, a non-Shutterfly user, alleged that "[t]here are likely tens of thousands of individuals who, while residing in Illinois, had their photos uploaded to Shutterfly."[67]

The *Shutterfly* court found that allegation sufficient to establish personal jurisdiction. The court reasoned that: (1) Shutterfly operates a number of websites that provide digital photo storage and sharing services that are available in all fifty states; (2) Shutterfly is accused of violating is an Illinois statute and stems out of its contact with Illinois

---

59 *Id.* ¶ 22.

60 *Id.* ¶ 8.

61 Defendant Facebook, Inc.'s Memorandum of Law in Support of its Motion to Dismiss, *Gullen v. Facebook.com, Inc.,* No. 1:15-cv-07681 (N.D. Ill. Aug. 31, 2015), ECF No. 20.

62 *Id.*

63 Order on Motion to Dismiss, *Gullen v. Facebook.com, Inc.,* No. 1:15-cv-07681 (N.D. Ill. Jan. 1, 2016), ECF No. 37.

64 Complaint ¶ 10, *Gullen v. Facebook.com, Inc.,* No. 1:15-cv-07681 (N.D. Ill. Aug. 31, 2015), ECF No. 1.

65 *Id.* ¶ 22.

66 *Illinois v. Hemi Grp. LLC*, 622 F.3d 754, 760 (7th Cir. 2010) (stating operation of interactive website insufficient to create specific jurisdiction). The Court never determined whether Gullen could state a claim for relief under BIPA, leaving companies guessing.

67 First Amended Class Action Complaint ¶10, *Norberg v. Shutterfly, Inc.*, No. 1:15-cv-05351 (N.D. Ill. June 23, 2015), ECF No. 6.

residents; and (3) because Norberg is a private Illinois resident, there is a strong interest in adjudicating the matter locally.

The Shutterfly decision stands in sharp contrast to the Facebook decision and Seventh Circuit precedent, which has rejected the notion that an online merchant's operation of an interactive site is sufficient to confer specific jurisdiction on it in every state from which the site can be accessed.

B. The Supreme Court's Recent Ruling in Spokeo May Slow the Growth of BIPA Class Action Suits

1. The *Smarte Carte* Suit

Another defense is lack of subject matter jurisdiction. At a high-level, subject matter jurisdiction refers to the court's authority to hear a particular case. In federal court, a plaintiff must establish Article III standing. Without it, the federal court does not have subject matter over the case.

The Supreme Court recently clarified a plaintiff's requirement to establish Article III standing. In *Spokeo, Inc. v. Robins*, the Supreme Court held that to establish Article III standing, a plaintiff must allege "concrete" harm—which the Supreme Court described as harm that is "real" and "not abstract."[68] The Ninth Circuit held previously that a "statutory violation automatically establishes standing," but the Supreme Court held that the allegation of a statutory violation does not by itself suffice to meet the "real" harm standard. *Spokeo* thus holds that a plaintiff has standing to bring a statutory claim only when the asserted violation encompasses an allegation of concrete harm—either because (1) an element of the cause of action requires proof of such a harm, and the plaintiff alleges facts sufficient to establish that element; or (2) the plaintiff separately alleges facts establishing a concrete harm.[69]

The Northern District of Illinois relied recently on *Spokeo* to dismiss a putative BIPA class action.[70] That suit concerns Smarte Carte's alleged collection, storage, and use of biometric data without consumer consent in violation of BIPA.[71] The complaint alleges that in 2008, Smarte Carte introduced electronic lockers for rent. Unlike traditional rental lockers that require a key, Smarte Carte's electronic lockers scan, collect, and record the renter's fingerprint at the time of rental; the renter unlocks the locker using that recorded fingerprint.[72] The plaintiff McCollough allegedly used and paid for an electronic locker five times in 2015.[73] She contends that, in violation of BIPA, Smarte Carte did not inform renters in writing that their biometric identifiers or biometric information was being collected or stored, for how long such information would be

---

68 *Spokeo, Inc. v. Robins,* 136 S. Ct. 1540, 1548 (2016).

69 *Id.* at 1549-50.

70 *McCollough v. Smarte Carte, Inc.,* No. 16-cv-03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016).

71 *Id.* at *1.

72 *Id.*

73 *Id.*

stored, or make available a written policy disclosing when such information will be destroyed permanently.[74]

Smarte Carte filed a motion to dismiss and argued that the court lacked subject matter jurisdiction.[75] Principally, Smarte Carte argued that "[n]owhere in the Complaint does Plaintiff contend that she suffered any harm, loss or injury."[76] Plaintiff's alleged BIPA violations, without more, are insufficient to confer standing under Article III of the U.S. Constitution.[77]

The Court agreed. "This Court finds that plaintiff has alleged the sort of bare procedural violation that cannot satisfy Article III standing."[78] McCollough did not allege any harm that resulted from the alleged violation.[79] "Even without prior written consent to retain, if Smarte Carte did indeed retain the fingerprint data beyond the rental period, this Court finds it difficult to imagine, without more, how this retention could work a concrete harm."[80] The court went on to ask: "How can there be an injury from the lack of advance consent to retain the fingerprint data beyond the rental period if there is no allegation that the information was disclosed or at risk of disclosure?"[81]

2. The *Original Facebook* Suit and The *Take-Two* Suit

Facebook, after failing to dismiss the Plaintiffs' putative class action suit on 12(b)(6) grounds,[82] filed in June 2016 a motion to dismiss for lack of standing based on *Spokeo*. According to Facebook, Plaintiffs allege that Facebook violated BIPA because it failed to develop a written policy governing the retention and destruction of documents and failed to notify and obtain informed written consent from the individuals whose biometric information Facebook purportedly collected. But, Plaintiffs did not allege that they have been harmed by these supposed technical violations of BIPA.[83] Facebook's motion to dismiss for lack of subject matter jurisdiction is still pending.

Take-Two is advancing a similar argument in its defense of a BIPA class action filed against it. Take-Two develops and publishes basketball-themed video games NBA 2K15

---

74 *Id*. at *2.

75 *Id*. at *2-3.

76 Defendant Smarte Carte, Inc.'s Memorandum of Law in Support of Motion to Dismiss at 2, *McCollough v. Smarte Carte, Inc.*, No. 16-cv-03777 (N.D. Ill. May 6, 2016), ECF No. 13.

77 "Any person ***aggrieved*** by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal court against an offending party." 740 Ill. Comp. Stat. § 14/20 (2008) (emphasis added).

78 *McCollough,* 2016 WL 4077108, at *3.

79 *Id*.

80 *Id*. at *4.

81 *Id*. The Court also found that the Plaintiff failed to state a claim under BIPA. BIPA provides that "[a] ny person aggrieved" has a right of action. The Court interpreted "aggrieved" to require a showing of injury; since McCollough has not alleged any facts showing that her rights have been adversely affected by the purported BIPA violations, she has not stated a claim.

82 *See* Part Two, *supra*.

83 Motion to Dismiss for Lack of Subject Matter Jurisdiction, *In re Facebook Biometric Information Privacy Litigation*, No. 15-cv-03747-JD (N.D. Cal. June 29, 2016), ECF No. 129.

and NBA 2K16. Each game contains a "MyPlayer" feature which allows users to create a personalized basketball avatars by taking a photograph.[84]

In *Take-Two,* Plaintiffs Ricardo Vigil and his sister Vanessa Vigil sued Take-Two for BIPA violations. They allege that this process violates BIPA: "Take-Two has created, collected and stored 'scans of face geometry' (or 'face templates')–highly detailed geometric maps of the face–from thousands of Illinois residents. Both the NBA 2K15 and NBA 2K16 video games are equipped with software that, in combination with a camera attached to a personal computer or a game console, operates to extract and analyze data from the points and contours of the face of an individual playing the game, and thereafter creates a virtual player with a personally identifying facial rendition. Each face template, on which each rendition is based, is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person."[85]

Take-Two's motion is predicated not on whether Take-Two violated BIPA, but whether the plaintiffs can establish that they have been harmed by any purported violations. To support a damages claim, Ricardo Vigil claims he would not have purchased the NBA 2K15 video game if he knew that one of the games features violates BIPA. Both Ricardo and his sister allege that Take-Two misappropriates valuable biometric data and that they face an increased risk that their biometric data may be compromised in the future. Take-Two denounces that any of these allegations can support standing under Article III, or even state a claim for relief under BIPA itself, as neither plaintiff can demonstrate he or she is an aggrieved party as BIPA requires.[86] Take-Two's motion to dismiss for lack of subject matter jurisdiction is also pending.

If district courts follow *Smarte Carte,* then BIPA class action suits may be limited as plaintiffs will be required to allege concrete harm resulting from the alleged BIPA violation, and not merely a BIPA violation itself.

3. The Arbitration Agreement Defense?

Snapchat became the latest social media company purportedly using facial recognition technology to face suit under BIPA. Plaintiffs Jose Luis Martinez and Malcolm Neal, both Snapchat users, filed suit in California state court May 2015.[87] They alleged that: (i) Snapchat's "Lenses" feature relies on facial recognition technology to allow users to add real-time special effects and sounds to photographs; (ii) scans a user's face each time he or she uses Lenses; and (iii) collects, stores, and uses geometric data

---

84 Memorandum of Law of Defendant Take-Two Interactive Software, Inc. in Support of Motion to Dismiss the Second Amended Complaint, *Santana v. Take-Two Interactive Software, Inc.*, No. 1:15-cv-08211-JGK (S.D.N.Y. July 29, 2016), ECF No. 49.

85 Second Amended Complaint ¶ 5, *Santana v. Take-Two Interactive Software, Inc.*, No. 1:15-cv-08211-JGK (S.D.N.Y. July 15, 2016), ECF No. 43.

86 Memorandum of Law of Defendant Take-Two Interactive Software, Inc. in Support of Motion to Dismiss the Second Amended Complaint, *Santana v. Take-Two Interactive Software, Inc.*, No. 1:15-cv-08211-JGK (S.D.N.Y. July 29, 2016), ECF No. 49.

87 Complaint, *Martinez v. Snapchat, Inc.*, No. 2:16-cv-05182-SVW (C.D. Cal. May 23, 2016), ECF No. 1-1.

relating to the unique points and contours (*i.e.,* biometric identifiers) of each face without consent, in violation of BIPA.[88]

In July, Snapchat removed the case to the Central District of California,[89] presumably to be able to assert an Article III challenge following *Spokeo.* In August, Snapchat filed a motion to compel arbitration, arguing that all Snapchat users, including plaintiffs, expressly agreed under Snapchat's Terms of Use to individually arbitrate all claims and disputes arising in connection with their use of any Snapchat service.[90]

Snapchat's arbitration notice includes a waiver to participate in class-action lawsuits or classwide arbitrations.[91] Snapchat's motion to compel arbitration also noted that Lenses does not use facial recognition technology to place these special effects. "Instead it uses object recognition technology, which allows Lenses to identify a nose as a nose or an eye as an eye, but does not—and cannot—identify a nose or an eye, let alone a whole face, as belonging to any specific person."[92] On August 30, 2016, plaintiffs voluntarily dismissed their complaint without prejudice.[93]

Just eight days after Snapchat filed its motion to compel arbitration, asserting that the plaintiffs expressly waived their right to class-action litigation and classwide arbitration, the plaintiffs dismissed their suit voluntarily. Because the *Snapchat* suit was dismissed voluntarily, it is unknown how the Court would have ruled on Snapchat's motion to compel arbitration. Clearly, however, if a plaintiff cannot file a class action, then the appeal of BIPA to plaintiffs' lawyers, and the per violation statutory penalties BIPA provides, dwindles.

V. PART FOUR: THE RISE OF CLASS ACTION SUITS AGAINST SOCIAL MEDIA COMPANIES BASED ON THEIR ALLEGED SCANS OF PHOTOGRAPHS AND ITS POTENTIAL IMPACT ON BIOMETRIC LEGISLATION

A. The Proposed Amendments to BIPA

On May 26, 2016, in response to the floodgates of photograph-based facial recognition BIPA class action suits, Illinois Senator Terry Link filed a proposed amendment to BIPA.[94]

---

88 *Id.* ¶ 33.

89 Notice of Removal, *Martinez v. Snapchat, Inc.*, No. 2:16-cv-05182-SVW (C.D. Cal. July 14, 2016), ECF No. 1.

90 Motion to Compel Arbitration, *Martinez v. Snapchat, Inc.*, No. 2:16-cv-05182-SVW (C.D. Cal. Aug. 22, 2016), ECF No. 21.

91 *Id.*

92 *Id.*

93 Notice of Voluntary Dismissal, *Martinez v. Snapchat, Inc.*, No. 2:16-cv-05182-SVW (C.D. Cal. Aug. 30, 2016), ECF No. 29.

94 Linn Foster Freedman, *Proposed amendment to Illinois biometrics privacy law introduced then stalled,* DATA PRIVACY + SECURITY INSIDER (June 2, 2016), https://www.dataprivacyandsecurityinsider.com/2016/06/proposed-amendment-to-illinois-biometrics-privacy-law-introduced-then-stalled/.

In pertinent part, Senator Link's proposed amendments sought two main changes. First, it expressly excluded both physical and digital photographs from BIPA's definition of "biometric identifier." Second, it added a new defined term, "scan," and limited the definition of "scan" to in-person scans.

TERM	BIPA	PROPOSED AMENDMENT
"Biometric Identifier"	**"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 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, <u>physical or digital</u> 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 Information"	**"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."	**"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" and "biometric identifier" do ~~Biometric information does~~ not include information derived from items or procedures excluded under the definition of biometric identifiers."
"Scan"	**N/A**	**"Scan"** means data resulting from an in-person process whereby a part of the body is traversed by a detector or an electronic beam.

By excluding from the definition of "biometric identifier" physical and digital photographs and clarifying that the term "scan" must occur in-person, the proposed BIPA amendment would have effectively abrogated BIPA claims related to the collection of user faceprints by online services. Not surprisingly, the proposed BIPA amendment sparked debate.

Critics of the proposed BIPA amendment were angered by the timing, substance, and intent behind the proposed amendment. Senator Link made his proposal just before the Memorial Day weekend and attached the bill to the end of an unrelated bill regarding unclaimed property. Critics also believed the proposed amendment would nullify biometric protections. It is common in biometrics for scanning to be of an image or photograph. The proposed amendment "retroactively removes the consumer protections of [BIPA] and renders the Act effectively null," by changing the technical definition of biometric scans as to render BIPA inapplicable to actual biometrics.[95] "To purposefully and specifically exclude photographs and digital photographs, as the proposed amendment does, means BIPA will essentially not apply to biometrics due to how biometric analytical processes work."[96] Critics believed further that the proposed BIPA amendment was not intended to secure biometric data, but was instead submitted in response to lobbying efforts from social media companies such as Facebook and Google:

> We suspect that the proposed Amendments were introduced in an effort to immunise Facebook, Google, and others, from liability in the lawsuits they are facing. That's because two federal courts have looked at whether BIPA regulates facial recognition technology as applied to uploaded photographs (in cases against Shutterfly and Facebook) and both federal courts have held that the statute unambiguously regulates the activity. It appears that the proposed Amendments are an effort to achieve through new legislation what these social media companies have been unable to achieve through the courts. Absent a retroactively applied amendment to BIPA, the pending lawsuits against Facebook and Google should proceed to trial. An 'in person scan' using a 'detector' or 'electronic beam' is not how companies are actually obtaining consumers' biometric data in the real world. If the intermediation of a photograph excused all subsequent processing into a biometric identifier, as the Amendments would have done, then practically all biometric data gathered and stored against consumers' wishes would be free from regulation and thus wholly permitted. Simply stated, the Amendments would have entirely swallowed the rule against unauthorised collection of biometric identifiers, rendering the statute and its promises of protection entirely hollow.[97]

Proponents of the amendment argue that Senator Link's proposal did nothing more than clarify BIPA's intent. Senator Link's proposed amendment merely adds the words "physical or digital" to the word "photograph" to make it clear that photographs are

---

95 Letter from Abraham Scarr, Dir. of Ill. Public Interest Research Grp., to Sen. Bliss (May 27, 2016), https://www.eff.org/files/2016/06/07/2016-05-27_letter_-_il-pirg_against_il_hb_6074_0.pdf.

96 Letter from Pam Dixon, Exec. Dir. of World Privacy Forum, et al., to Sen. Bliss (May 27, 2016), https://www.eff.org/files/2016/06/07/2016-05-27_letter_-_wpf_against_il_hb_6074_0.pdf.

97 Frank S. Hedin and David P. Milian, *BIPA Amendment Put on Hold After Backlash from Privacy Advocates,* Carey Rodriguez Attorneys (June 2, 2016), http://www.careyrodriguez.com/blog/bipa-amendment-put-on-hold-after-backlash-from-privacy-advocates/.

not included in the law. The amendment further includes a definition of "scan," which clarifies that a scan included in the law is "an in-person process whereby a part of the body is traversed by a detector or an electronic beam."[98] These changes would in effect confirm that the scanning of a digital photograph of a person's face is not covered by the law, and proponents argued that these changes are merely clarifications to the definitions in the existing law and are consistent with the intent of the law.[99]

The next day, Senator Link announced that the amendment was put on hold, but did not specify why.[100]

B. Other State Biometric Statutes Define Biometric Information Differently than BIPA

1. Texas' Biometric Statute Does Not Expressly Exclude Photographs from Its Definition of Biometric Information

The surging popularity of photograph-based facial recognition BIPA suits against Facebook, Google, and Snapchat begs the question: What about the biometric statutes of other states?

Texas enacted its biometric statute, the Capture or Use of Biometric Identifier ("CUBI"), in 2009.[101] BIPA and CUBI have many similarities. Like BIPA, CUBI prohibits the collection of biometric information without informed consent. Under CUBI, "[a] person may not capture a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2) receives the individual's consent to capture the biometric identifier."[102] And like BIPA, CUBI defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[103]

BIPA and CUBI, however, are not without differences. CUBI does ***not*** expressly exclude photographs from its definition of biometric identifier. And under CUBI, biometric identifiers include "record[s]" (as opposed to just "scans") of hand and face geometry. Arguably, CUBI has a broader reach than BIPA.

Certainly companies such as Google and Facebook have millions of users in Texas. Unquestionably, thousands of those users upload photographs upon which Google and Facebook scan and identify other users found in them. Unlike BIPA, however, CUBI is not subject to class action suits. That is because CUBI is enforceable only by the state attorney general. That CUBI does not allow for private rights of action seems to be the main reason why such suits are not prominent.

---

98 Linn Foster Freedman, *Proposed amendment to Illinois biometrics privacy law introduced then stalled,* Data Privacy & Security Insider (June 2, 2016), https://www.dataprivacyandsecurityinsider.com/2016/06/proposed-amendment-to-illinois-biometrics-privacy-law-introduced-then-stalled/.

99 *Id.*

100 *Id.*

101 Tex. Bus. & Com. Code Ann. § 503.001 (2009).

102 *Id.* § 503.001(b).

103 *Id.* § 503.001(a).

	BIPA	CUBI
Prohibit Collection of Biometric Identifiers without informed consent?	Yes	Yes
Definition of "biometric identifier"	A retina or iris scan, fingerprint, voiceprint, or ***scan*** of hand or face geometry	A retina or iris scan, fingerprint, voiceprint, ***or record*** of hand or face geometry
Definition of "biometric identifier" expressly exclude photographs?	Yes	No
Private Right of Action?	Yes	No

2. Unique Identifying Information Derived From Photographs Would Appear to Fall Under the Plain Text of Proposed Biometric Privacy Statutes in Other States

Proposed biometric privacy statutes in other states have varying definitions of "biometric information." For example, Alaska has a proposed biometric privacy statute that defines broadly **"biometric data"** as "fingerprints, handprints, voices, iris images, retinal images, vein scans, hand geometry, finger geometry, or other physical characteristics of an individual."[104] It defines further **"biometric information"** as "data used in a biometric system," and defines **"biometric system"** as an automated system that [1] captures biometric data from an individual's biometric information [2] extracts, processes, and stores that captured biometric data, and [3] compares the extracted biometric data from the individual with stored biometric data for recognition of the individual.[105] The proposed Alaska law does not apply to the collection, retention, analysis, disclosure, or distribution of "photographs," unless the photograph is collected for use in a biometric system.

Based on the text of the proposed statute, if the allegations in the existing BIPA photograph-based facial recognition BIPA suits are true, it would appear that uploading photographs to Facebook or Google Photos would be considered a photograph collected for use in a biometric system because:

[1] The defendants allegedly capture biometric data from an individual's biometric information;

[2] The defendants allegedly extract and processes that data; and

---

104 H.B. 96, 29th Leg. (Alaska 2015).

105 *Id.* § 18.14.090.

[3] The defendants allegedly compare the extracted data with an existing biometric data database to recognize the individual.

Before going dormant last September, California proposed a bill that would have extended the scope of California's data security law to biometric data. California's proposed amendment defined "biometric information" as "data generated by automatic measurements of an individual's fingerprint, voice print, eye retinas or irises, identifying DNA information, or unique facial characteristics, which are used by the owner or licensee to uniquely authenticate an individual's identity."[106]

New York's pending amendment defines biometric information as " . . . data generated by automatic measurements of an individual's physical characteristics, which are used by the owner or licensee to authenticate an individual's identity[.]"[107]

Under either definition, it would again appear that algorithms taking automatic measurements of a person's unique biological characteristics, even though through a photograph, would constitute biometric information. Neither of the proposed bills have an exclusions for photographs or information derived from photographs.

VI. PART FIVE: THE EFFECT THE UNCERTAIN BIOMETRIC LEGAL LANDSCAPE HAS ON PROTECTING GENUINE BIOMETRIC INFORMATION

The practical applications of facial recognition technology are seemingly limitless. Facial recognition technology offers convenience. For instance, Apple has a patent for using facial recognition to unlock an iPhone. Apple's patent application touts the convenience of this feature: "[it] would eliminate some of the time-consuming steps for unlocking a device. As it stands now, users need to drag a slide bar and enter a password, steps that some might find inconvenient."[108]

Facial recognition technology provides security benefits too. Companies such as FaceFirst rely on facial recognition technology to provide security services to other companies. Among the many security benefits FaceFirst provides include sending descriptive alerts when an unwanted individual walks into your building; flagging individuals who have caused problems previously; monitoring the movement of people in your facility to ensure that no one is in an unauthorized area; and eliminating the possibility of misidentification of criminals who are using false identification.[109]

But in a consumer driven world, arguably facial recognition technology's most valuable use will be targeted advertising; it can be used to track the likes and dislikes of specific individuals. For instance, companies like Affectiva use facial recognition

---

106 A.B. 83, 2015-2016 Leg., Reg. Sess. (Cal. 2015).

107 A.B. 06866, 2015-2016 Leg., Reg. Sess. (N.Y. 2015).

108 Abin Sam, *Now Unlock your Devices with a Selfie!,* Khurana & Khurana (July 20, 2015), http://www.khuranaandkhurana.com/2015/07/20/now-unlock-your-devices-with-a-selfie/; *see* U.S. Patent No. 8,994,499.

109 FaceFirst, http://www.facefirst.com/services/commercial-security; http://www.facefirst.com/services/law-enforcement (last visited October 6, 2016).

technology to measure and analyze the moment-to-moment facial expressions of people watching videos. To marketers, a person's visceral response to a video can be more accurate than their verbal description.[110] It should come as no surprise then that the facial recognition market is expected to grow to $6.19 billion by 2020.[111] The use of biometrics will only continue to grow.

The dearth of consumer privacy biometric statutes, however, and the corresponding disconnect between the judicial interpretation of BIPA and its plain text, greatly impacts biometrics. This uncertain landscape has allowed savvy class action attorneys to target social media giants such as Facebook and Google in seeking multi-million dollar judgments against them. Are these suits, which allege BIPA consent violations, and not that the purported biometric information has been compromised, intended to safeguard biometric information?

Ironically, BIPA and CUBI were enacted nearly one decade ago, which is an eternity when it comes to technology. Although at the forefront of the biometric information privacy and consumer interface, companies that do collect, store, and use biometric information are still uncertain of their legal obligations. Accordingly, these companies will likely focus on how to avoid suit as opposed to protecting genuine biometric information. Until the laws catch up with the technology, this discord will persist.

It may take many years for BIPA to become settled and many more for federal and state laws to catch up with biometric technology generally. In the interim, companies in the biometric industry should keep abreast of the following:

1. What other states are on the verge of passing biometric legislation?
2. Are any states proposing laws that would generate biometric privacy litigation?
3. Are there any proposed federal laws that would generate biometric privacy litigation?
4. Are there any proposed amendments to existing biometric privacy statutes, like BIPA and CUBI?
5. From what sources are the purported biometric information derived? Photographs?
6. Are the persons filing suit users or non-users of the company's services?
7. Does the state statute allow for a private right of action, or can only the State Attorney General file suit?
8. In what state is the private entity being sued? Is there personal jurisdiction?
9. In what court (state v. federal) is the private entity being sued? Can the suit be removed to federal court?

---

110 E.J. Schultz, *Facial-Recognition Lets Marketers Gauge Consumers' Real Responses to Ads,* AdvertisingAge (May 18, 2015), http://adage.com/article/digital/facial-recognition-lets-marketers-gauge-real-responses/298635/.

111 Press Release, Facial Recognition Market worth $6.19 Billion by 2020, Markets and Markets, http://www.marketsandmarkets.com/PressReleases/facial-recognition.asp.

10. What harm is the plaintiff alleging? Does this harm rise to the standard required under *Spokeo* to grant the federal court subject matter jurisdiction? Does this harm rise to establish the plaintiff is an "aggrieved party" as required under BIPA?

11. Is there an arbitration agreement that waives class actions?

12. What constitutes notice before a company can collect or use biometric information?

13. What are the existing requirements for a company to store or destroy biometric information after it has been collected?

These questions may help provide companies with direction as they navigate in an ever evolving and uncertain biometric legal world.