New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication
Litigation
WWW.NYLJ.COM
MONDAY, FEBRUARY 22, 2016

Unique **Biometric Data** Creates Unique **Privacy Concerns**

BY NATASHA KOHNE, ISABELLE GOLD AND KAMRAN SALOUR

Forecast by some accounts to reach over $44 billion globally by 2021, the biometric technology market has created a fundamental shift in the way individuals worldwide are identified. It provides both instantaneous convenience and, if handled carefully, increased security to governments and consumers—whether through unlocking a smart phone, bypassing main security at the airport or protecting a country's borders. But there is also an inherent uneasiness about biometric identifiers: They are personal to a specific individual, permanent and indiscardable. It is not a password or pin that an individual chooses to create and can just as easily be changed. Indeed, the very benefits that biometric technology provides to consumers may also be its downfall. What happens if a database with biometric information is hacked? What is the impact of false negatives? How widespread should the use of biometric information be? The many unique attributes of biometric technology make the development of a proper legal framework vital.

Privacy Laws Lag Far Behind Technology

In spite of the rapid growth in biometric technology, and the need for appropriate legal guidelines, a misalignment of U.S. state and federal statutes exists, particularly concerning the most basic agreement on the definition of a biometric identifier. Both implemented biometric privacy statutes (Illinois, Texas) and proposed biometric privacy statutes (New York, California, and Texas) fail at defining clearly and uniformly biometric information. The only judicial interpretation defining in the commercial context a biometric identifier—issued just within the last two months—arguably broadened the definition of the term and cut against the plain language of the statute. This article examines the uncertain and unsettled definition of biometric information and the corresponding ambiguity it creates for

NATASHA KOHNE *is a partner at Akin Gump Strauss Hauer & Feld and co-leader of its cybersecurity, privacy and data protection and Middle East practices in the Abu Dhabi and San Francisco offices.* ISABELLE GOLD *and* KAMRAN SALOUR *are counsel in the firm's New York and Los Angeles offices, respectively.*

companies' seeking to satisfy their biometric privacy obligations. A company cannot begin to ensure the protection of biometric information if it is unclear what constitutes biometric information in the first place.

There is no doubt that if the benefits of biometric technology are to be maximized, the security of biometric information must be a priority. Adequate laws therefore must exist to protect this type of information. However, as with most emerging technologies, laws governing biometric technology lag behind the rapid development of this industry.

First, there is no uniform federal statute directed toward a private entity's collection, use, and storage of biometric information, and only a few states have enacted statutes addressing the protection of biometric information. Second, existing state statutes that do address biometric information are ambiguous and conflicting, especially with respect to the definition of biometric identifiers, making compliance difficult. Third, companies face exorbitant penalties for compliance failures, even for unintentional ones, making them susceptible to class action lawsuits. Where ambiguity lies, lawsuits tend to follow.

• Proposed and Existing Biometric Privacy Statutes Are Ambiguous and Lack Uniformity.

Existing Biometric Privacy Statutes' Definition of Biometric Information. In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA).[1] BIPA was the first statute to address biometric identifiers in a commercial setting. BIPA defines "biometric identifier" as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[2] This definition does not include, among other things, physical descriptions or *photographs*.[3] BIPA explicitly states that "biometric information" does not include "information derived from items [e.g., photographs] excluded under the definition of biometric identifiers."[4]

Texas's statute governing biometric identifiers, the "Capture or Use of Biometric Identifier" (CUBI), went into effect in 2009.[5] Like BIPA, CUBI defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[6] Unlike BIPA, however, CUBI does not explicitly exclude any categories of information from the definition of a biometric identifier.

As described above, BIPA and CUBI each set forth a seemingly specific definition of a biometric identifier. Moreover, based on the language of these two statutes, neither a photograph nor information derived from a photograph should constitute biometric information. Yet, as will be discussed further below, judicial interpretation of this statutory language has left the door open for a plaintiff to allege a BIPA violation based on the purported unauthorized collection of biometric information derived from a photograph.

Proposed Statutes in New York, Alaska, and California, Offer Different Definitions of Biometric Information. Further increasing the uncertainty surrounding the definition of "biometric information," proposed biometric privacy statutes drafted by states other than Illinois and Texas offer varying definitions.

For example, New York's proposed Data Security Act defines "biometric information" as "data generated by automatic measurements of an *individual's physical characteristics*, which are used … to authenticate the individual's identity."[7] Under this definition, it is unclear which "physical characteristics of an individual" will constitute biometric identifiers. This definition also conflicts with BIPA, which excludes certain physical characteristics from its definition of biometric information.

Alaska's proposed biometric privacy statute, "An Act Relating to Biometric Information,"[8] further clouds the picture. Alaska's proposal, like BIPA and CUBI, defines biometric data to include fingerprints and iris scans, which Alaska considers to be physical characteristics.[9]

California's proposed amendment to its existing data privacy statute only raises further questions. A state known to be at the forefront of digital privacy laws with strong constitutional privacy rights, California is seemingly behind in the area of biometric privacy; California's proposed amendment is currently dormant.[10]

California's proposed amendment nonetheless defines broadly "biometric information" as "data generated by automatic measurements of an *individual's biological characteristics* that are used … to authenticate an individual's identity, such as a fingerprint, voice print, eye retinas or irises, or other *unique biological characteristic*."[11] This definition extends biometric information beyond the relatively limiting definitions of BIPA and CUBI to include unique biological characteristics and data generated by automatic measurements of them.

But by expanding the scope of biometric information (and hence expanding the scope of biometric

protection), California's proposed amendment creates more confusion. It remains undefined what constitutes a unique biological characteristic, and whether "biological characteristics" under California's proposed amendment are synonymous with "physical characteristics" under New York's proposed law. The answers to these questions may never be known if California's proposed amendment remains dormant.

Existing and proposed statutes cannot define uniformly and unambiguously biometric information. (See table on page S11).

Statute	Biometric Identifier Means...	Certain Unanswered Questions
BIPA	A retina or iris scan, fingerprint, voiceprint, or hand scan or face geometry.	Is a photograph or information derived from a photograph considered a "biometric identifier?"
CUBI	A retina or iris scan, fingerprint, voiceprint, or hand scan or face geometry.	Can a record of hand or face geometry be derived from a photograph?
NY Proposed Statute	Data generated by automatic measurements of an individual's physical characteristics to authenticate an individual's identity.	What are "automatic measurements?" Are "physical characteristics" identical to the physical characteristics expressly excluded under BIPA? Or are "physical characteristics" synonymous with "biological characteristics" under CA's Proposed Statute?
AK Proposed Statute	Fingerprints, handprints, voices, iris images, retinal images, vein scans, hand geometry, finger geometry, or other physical characteristics of an individual.	What "other physical characteristics" are biometric information.
CA Proposed Statute	Data generated by automatic measurements of an individual's biological characteristics that are used to authenticate an individual's identity, such as a fingerprint, voice print, eye retinas or irises, or other unique biological characteristic.	What are "automatic measurements?" Are "biological characteristics" synonymous with "physical characteristics" under NY's proposed statute?

• Implemented and Proposed Biometric Privacy Statutes Impose High Statutory Penalties for Non-Compliance and Leave Companies Vulnerable to Suit.

The varying, conflicting and often ambiguous definitions of "biometric information" in existing and proposed biometric statutes create significant risk for companies; as a result, these companies may incur significant civil penalties for alleged noncompliance with the various statutes at play.

BIPA authorizes statutory penalties ranging from $1,000 for a negligent violation, to $5,000 for an intentional violation.[12] CUBI imposes civil penalties of up to $25,000 per violation.[13] By comparison, the highly litigated federal Telephone Consumer Protection Act authorizes only a $500 per violation penalty.[14]

New York's proposed statute empowers the New York Attorney General to impose civil penalties of $250 for each person, up to a maximum of $10 million. For knowing and reckless violations, penalties can escalate to $1,000 for each person, up to a maximum of $50 million.[15] Alaska's proposed statute levies a $5,000 penalty under certain conditions.[16] California's proposed amendment does not impose a civil penalty or allow for liquidated damages.[17]

The magnitude of these statutory penalties may be tempered by the Supreme Court's forthcoming ruling in *Spokeo v. Robins*,[18] where the court will decide whether a plaintiff has standing to assert only a statutory violation where no actual "injury-in-fact" occurred. Although the court will address that issue in connection with a suit brought under the Fair Credit Reporting Act, if the court holds that standing does require an actual injury-in-fact, suits under biometric statutes may slow and help shield companies from the cost of non-compliance.

• Judicial Interpretation of Biometric Information Under BIPA.

Given the current state of biometric privacy law and the steep civil penalties that are presently available, it is not surprising that plaintiffs have asserted statutory violations in the social media context, where violations can multiply quickly and corresponding civil penalties can escalate to the millions.

Perhaps it is because BIPA was the first biometric privacy statute, or the hotbed of plaintiffs' attorneys in Chicago that have been known to challenge other privacy suits, but to date, the only suits to have alleged a private entity's violation of a biometric privacy statute are those asserted against BIPA.

In 2015, three class action lawsuits alleging BIPA violations were

filed against Facebook.[19] These suits, which have since been consolidated and transferred to the Northern District of California, present a challenge to Facebook's omnipresent "Tag Suggestions" feature, which allegedly scans photographs uploaded by a Facebook user and then identifies faces appearing in those photographs. The class action plaintiffs allege that Facebook's Tag Suggestions feature violates BIPA because it obtains this biometric identifier without a Facebook user's knowledge or consent.[20] On Oct. 9, 2015, Facebook filed a motion to dismiss arguing that the plaintiffs cannot state a claim under BIPA because BIPA expressly excludes from its definition of "biometric identifier" photographs and any information derived from those photographs.[21] The motion to dismiss is pending.[22]

The outcome of Facebook's motion to dismiss will likely be impacted by the recent ruling in another class action lawsuit alleging a violation of BIPA: *Norberg v. Shutterfly*, No. 15-cv-05351 (N.D. Ill. June 17, 2015). In *Norberg*, the plaintiff alleged that Shutterfly violated BIPA by creating, collecting, and storing millions of "face templates" without consent. Shutterfly allegedly created these face templates by using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces appearing in photos uploaded by their users. Each face template is unique to a particular individual.

Shutterfly filed a motion to dismiss, arguing that BIPA excludes photographs and information derived from photographs from the definition of biometric information. Marking the first judicial interpretation of BIPA, the court acknowledged that BIPA's definition of biometric information excludes photographs and information derived from photographs. The court noted further that to survive a motion to dismiss, the alleged claim must actually suggest that the plaintiff has a right to relief. It would appear therefore that the plaintiff's claim should fail since the plaintiff cannot suggest a right to relief under BIPA.

But the court nonetheless found that the plaintiff stated a claim for relief under BIPA by alleging that Shutterfly is using the plaintiff's personal face pattern to recognize and identify him in photographs posted to websites.[23]

The long-term ramifications of the *Shutterfly* decision are unclear; however, in the short-term, the decision puts: (1) further uncertainty in BIPA's definition of biometric information; (2) companies at risk for suit; and (3) consumers' biometric information at risk.

Open Questions

The infancy and dearth of biometric statutes, and their corresponding lack of judicial interpretation, create uncertainty for companies that use biometric information. Companies cannot effectively protect biometric information without a clear and consistent definition of biometric information. This uncertain statutory landscape has opened the door to savvy class action attorneys whose focus is arguably not on protecting an individual's biometric information but on capitalizing from nascent and ineffective biometric privacy laws. In turn, companies focus not on protecting biometric information, but on avoiding being sued. In the end, biometric privacy laws do little to achieve their intended purpose of protecting biometric information.

1. 740 ILL. COMP. STAT. §14/1 et seq. (2008).
2. Id., §14/10.
3. Id. (emphasis added).
4. Id.
5. TEX. BUS. & COM. CODE ANN. §503.001 (2009).
6. Id., §503.001(a).
7. Assemb. B. 6866, 2015-2016 Reg. Sess. (N.Y. April 8, 2015); S.B. 4887, 2015-2016 Reg. Sess. (N.Y. April 22, 2015) (proposed amendment to N.Y. GEN. BUS. LAW §899-aa) (emphasis added).
8. H.B. 96, 29th Legis. §18.14.090 (AK 2015-2016).
9. Id.
10. https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201520160AB83.
11. Assemb. B. 83, 2015-2016 Reg. Sess. (CA Jan. 6, 2015) (proposed amendment to CAL. CIV. CODE §1798.81.5(d)(3)) (emphasis added).
12. 740 ILL. COMP. STAT. 14/20.
13. TEX. BUS. & COM. CODE ANN. §503.001(d).
14. 47 U.S.C. §227(b)(3)(B).
15. Assemb. B. 6866, 2015-2016 Reg. Sess. (N.Y. Apr. 8, 2015); S.B. 4887, 2015-2016 Reg. Sess. (N.Y. Apr. 22, 2015), §6.
16. H.B. 96, 29th Legis. §18.14.070 (AK 2015-2016).
17. CAL. CIV. CODE §1798.84(b).
18. No. 13-1339 (argued Nov. 2, 2015).
19. *Carlo Licata, Adam Pezen and Nimesh Patel v. Facebook (In re Facebook Biometric Information Privacy Litig.)*, Nos. 3:15-cv-03747-JD, 3:15-cv-03748-JD, 3:15-cv-03749-JD (N.D. Cal.).
20. *In re Facebook Biometric Information Privacy Litig.*, No. 3:15-cv-03747-JD, Consolidated Class Action Complaint, ¶ ¶ 3-5 (ECF No. 40, Aug. 28, 2015).
21. Id., Facebook's Motion to Dismiss (ECF No. 69, Oct. 9, 2015).
22. Another suit against Facebook, (*Gullen v. Facebook*, No. 1:15-cv-07681, (N.D. Ill. Aug. 31, 2015)), which also asserted BIPA violations based on Facebook's Tag Suggestions feature, was dismissed for lack of personal jurisdiction. (ECF No. 37, Jan. 21, 2016.)
23. Order on Shutterfly's Motion to Dismiss (ECF No. 41, Dec. 29, 2015).