By Kamran Salour

People take pictures — lots of them. And each year they take more. According to the New York Times, it is projected that in 2017 alone, people will take 1.3 trillion photographs. For context, a Deloitte study found that in 2000, individuals took 80 billion photos, then an all-time high. The reason for this substantial surge is simple: the ubiquity of camera-enabled phones.

With the ubiquity of camera-enabled phones — more precisely, the ease at which they allow users to snap, share and store digital photographs — individuals have amassed an enormous and ever-growing database of digital photos. Deloitte says that more than 5.1 billion photos are shared daily and more than 2.5 trillion photos will be shared or stored online by 2017.

The rapid rise in digital photography coincides with the uptick in the facial recognition market. The facial recognition market is expected to double to $6 billion by 2021. Its applications are infinite. In retail alone, companies can employ facial recognition technology to: identify valued customers; provide them a personalized shopping experience; and offer them conveniences like phone- and wallet-free purchases.

The inevitable ubiquity of facial recognition technology threatens the uniquity upon which it depends: the faceprint. Facial recognition technology detects a person's face, creates a faceprint by measuring the relative location of that person's facial features, and attempts to identify that person by comparing the faceprint to an existing faceprint database. Like all biometric identifiers, a faceprint's value is derived from its uniqueness; everyone has a distinctive faceprint. Unlike other biometric identifiers, a faceprint can be obtained without one's knowledge or consent. And because being photographed is relatively common, it is easy to forget that the more photographs people store online, the more likely that this biometric identifier will be exposed.

It is important then to strive for balance between adopting facial recognition technology and safeguarding biometric information. The law, unfortunately, provides little help in achieving this balance. There is no federal statute directed to biometric privacy. And only three states — Illinois, Texas and Washington — have enacted biometric privacy statutes.

But state statutes have failed to answer uniformly a threshold biometric privacy inquiry: When does a photograph-derived faceprint warrant privacy protection?

In 2008, Illinois enacted the Biometric Information Privacy Act. Under BIPA, a private entity must provide written notice and obtain written consent before collecting a biometric identifier. BIPA defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." BIPA's biometric identifier definition excludes "photographs or information derived from photographs." Texas' biometric statute adopted BIPA's biometric identifier definition; Texas' statute, however, does not exclude "photograph or information derived from photographs" from its definition.

Thus, based on the statutory language, it would appear that under BIPA, photograph-derived faceprints are unprotected. Appearances can be deceiving.

On at least three occasions, courts have interpreted BIPA's biometric identifier definition to include faceprints derived from scans of photographs.

In *Norberg v. Shutterfly*, Norberg sued Shutterfly, a photo-service company, which allows its users to store and organize photos. 1:15-cv-05351 (N.D. Ill. June 23, 2015). Norberg claimed that a Shutterfly user uploaded his photo to Shutterfly and Shutterfly subsequently stored Norberg's faceprint without his consent. Shutterfly argued that Norberg cannot state a claim under BIPA because "BIPA clearly and unequivocally states that photographs—and any information derived from photographs — are not within the scope of the law." The court disagreed: By alleging Shutterfly is using Norberg's personal face pattern to identify him in photographs, Norberg plausibly stated a claim.

Similarly, in *In re Facebook Biometric Information Privacy Litigation*, three plaintiffs alleged that Facebook's Tag Suggestions feature violates BIPA because it extracts a user's facial geometry without consent. 15-cv-03747-JD (N.D. Cal. May 5, 2016). Facebook argued that BIPA does not apply to photographs and information derived from photographs. The court disagreed and reasoned that "photographs" are better understood to mean paper photographs, not digital ones.

Finally, in *Rivera v. Google, Inc.*, the plaintiffs alleged that Google Photos creates "face templates" to identify individuals in uploaded photographs without their consent. Google moved to dismiss for failure to state a claim under BIPA. 1:16-cv-02714 (N.D. Ill. Feb. 27, 2017). The court held that the plaintiffs did state a claim under BIPA because for each face template, Google creates a set of biology-based measurements ("biometric") used to identify a person ("identifier"). And, a face template is one of BIPA's specified biometric identifiers–a "scan of … face geometry."

Thus far courts have interpreted BIPA's "biometric identifier" definition to include faceprints, even when they are derived from digital photographs. Texas' biometric statute has not undergone judicial interpretation. When Washington enacted its biometric privacy statute in 2017, it could have added uniformity to the question of whether a photograph-derived faceprint is a biometric identifier. It did not. Washington's "biometric identifier" definition excludes both physical and digital photographs.

Without uniformity, the optimal balance between facial recognition technology and photograph-derived faceprint protection cannot be reached.

Kamran Salour is an attorney with Callahan & Blaine in Santa Ana.