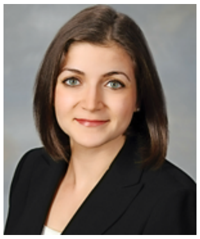
Bloomberg Law

Privacy and Security Law Report®

Illinois Biometric Privacy

In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA), the first state statute to regulate businesses' use of biometric identifiers and biometric information. Courts are currently focused on two main questions: the number of plaintiffs eligible to sue under BIPA; and whether facial recognition technologies commonly used by social media and other companies will become a main focus of biometric privacy litigation, the author writes.

The Illinois Biometric Information Privacy Act: A Case Law Update on Standing and Facial-Recognition Technologies



By Lara Tumeh

In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA), the first state statute to regulate businesses' use of biometric identifiers and biometric information (BII). 740 Ill. Comp. Stat. Ann. 14/1, *et seq*. BIPA generally requires private entities to (1) make their data retention policies publicly available; (2) give notice and receive consent before obtaining BII; (3) refrain from selling BII to third parties; (4) refrain from disseminating BII without prior written consent, absent certain exceptions; and (5) handle BII with reasonable care. The statute creates a private right of action and authorizes statutory damages up to $5,000 per violation, or actual damages, whichever is greater.

Lara Tumeh is a techology and privacy associate at Alston & Bird LLP in Atlanta.

Businesses are increasingly using biometrics in the context of financial and security transactions. With this rise of biometric-facilitated transactions have come a number of unique privacy and security risks. Biometrics are distinct from other identifiers, like social security numbers, used to access financial accounts or other sensitive information. They implicate not only informational but also bodily privacy. Moreover, if compromised, they cannot be changed, increasing the risk of identity theft. Illinois passed BIPA to address these unique concerns and enhance individual rights as the number of biometric-facilitated transactions grows.

BIPA gained significant attention in 2015, when a number of major BIPA cases were filed and the statute became the focus of biometric privacy litigation in the U.S. Since then, a number of state legislatures began considering biometric privacy bills similar to BIPA, including Alaska, Connecticut, Montana, New Hampshire and Washington.

As BIPA has become the focus of biometric litigation and legislation, recent case law interpreting BIPA has entered the spotlight. BIPA case law is currently focused on two main questions. First, if plaintiffs allege procedural violations of BIPA without alleging any resulting harm, do they have Article III and statutory standing? Second, are facial geometry templates—meaning scans of distinct facial measurements—created from photographs uploaded to the defendants' websites ''biometric identifiers'' within the meaning of BIPA?

Courts' answers to these two questions will determine the volume and stakes of BIPA litigation in coming years. The first question bears directly on the number of plaintiffs eligible to sue under BIPA and the rate at which case law interpreting BIPA develops. The second addresses whether facial recognition technologies commonly used by social media and other companies will become a main focus of biometric privacy litigation that proceeds beyond any standing hurdles.

Against this backdrop, two recent BIPA cases are worth examining: *Vigil v. Take-Two Interactive Software, Inc.*, No. 15-cv-8211 (S.D.N.Y. Jan. 30, 2017), which addresses the first question described above, and *Rivera v. Google Inc.*, No. 16-cv-02714 (N.D. Ill. Feb. 27, 2017), which addresses the second.

Recent BIPA Case Law

Standing The most significant threshold question in current BIPA litigation as of yet is whether plaintiffs alleging procedural violations of BIPA have Article III and statutory standing. The U.S. District Court for the Southern District of New York recently examined this question in *Vigil*. *Vigil* involved a defendant—Take-Two Interactive Software, Inc.—that published, developed and distributed video games. One feature of these games called ''MyPlayer'' allegedly allowed players to undergo a 15-minute face scanning process so the game could create ''personalized basketball avatars,'' or virtual players based on a 3D rendition of their own faces. Before using this feature, a player was required to agree to the following statement: ''Your face scan will be visible to you and others you play with and may be recorded or screen captured during gameplay.'' *Vigil*, No. 15-cv-8211 at 10. Avatars were allegedly available to third-party players only if the gamer chose to play in multiplayer mode.

The plaintiffs brought a putative class action under the Class Action Fairness Act. They alleged Take-Two violated BIPA's storage and dissemination requirements by failing to publicly provide a retention schedule for permanently destroying their biometric identifiers, by failing to transmit their biometric identifiers with industry-standard reasonable care and by profiting from the plaintiffs' biometric identifiers. They claimed Take-Two also violated BIPA's notice and consent provisions, alleging the notice received and consent obtained was insufficient ''because the MyPlayer feature terms and conditions did not specifically disclose that their faces constituted biometrics, the purpose of the scanning, or the length of the face scan retention period; because the plaintiffs' consent to use the MyPlayer feature was not embodied in a writing; and because Take-Two did not publish a biometric retention schedule.''

The district court held the plaintiffs lacked Article III standing under *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), *as revised* (May 24, 2016), and Second Circuit progeny. In *Spokeo*, the U.S. Supreme Court instructed that a plaintiff cannot ''allege *a bare procedural violation, divorced from any concrete harm*, and satisfy the injury-in-fact requirement of Article III.'' *Id.* at 1549 (emphasis added). It noted, ''[d]eprivation of a *procedural right without some concrete interest* that is affected by the deprivation . . . is insufficient to create Article III standing.'' *Id.* (emphasis added and quotations omitted).

Applying *Spokeo* and progeny to *Vigil*, the district court reasoned ''the first task is to identify any 'concrete interests' protected by the BIPA.'' *Vigil*, No. 15-cv-8211 at 22. It held the ''core object'' of BIPA is ''to curb potential misuse of biometric information collected by private entities'' such that ''when an individual engages in a biometric-facilitated transaction, the private entity protects the individual's biometric data, and does not use that data in a way not contemplated by the underlying transaction.'' *Id.* at 3. The court concluded the plaintiffs failed to establish standing because they did not allege procedural harms leading to use other than as contemplated by the underlying transaction.

As to the alleged violations of BIPA's storage and dissemination provisions more specifically, the court held that the plaintiffs failed to establish ''an imminent risk that their biometrics could actually be misused, and there has been no event, such as the data theft . . . that could make any such risk rise above the abstract level.'' It added, ''[a]t best, the plaintiffs' allegations are that Take-Two's storage and dissemination practices have subjected their facial scans to an 'enhanced risk of harm' of somehow falling into the 'wrong hands,' which is too abstract and speculative to support standing.'' *Id.* at 25-26.

As to the alleged violations of BIPA's notice and consent provisions, it similarly reasoned that the ''alleged failure to give the plaintiffs more extensive notice and consent is not a material risk to a concrete BIPA interest where no material risk of biometric data misuse ever materialized.'' It noted, ''[u]nlike statutes where the provision of information about statutory rights, or matters of public concern, is an end itself, the BIPA's notice and consent provisions do not create a separate interest in the right-to-information, but instead operate in support of the data protection goal of the statute[:] . . . the fulfillment of the transaction in question.'' *Id.* at 29-30.

Finally, the court held the plaintiffs also lacked statutory standing because they failed to demonstrate any harm. The court reasoned that, in granting a private right of action specifically to ''aggrieved'' individuals, the statute ''limits a private right of action to a party that can link an injury to a statutory violation.'' *Id.* at 47.

Vigil is at least the second court to conclude a BIPA plaintiff lacked Article III and statutory standing. *See, e.g.*, *McCollough v. Smarte Carte, Inc.*, No. 16-cv-03777 (N.D. Ill. Aug. 1, 2016) (concluding the plaintiff lacked constitutional standing and asking, ''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?''); *id.* at *4 (holding the plaintiff lacked statutory standing). It is significant because, if adopted by other courts, it may significantly reduce BIPA litigation on the merits. With less litigation on the merits will come less case law interpreting BIPA and, as a result, less certainty regarding the scope of the statute.

the Illinois legislature is considering an amendment that would carve out face templates from the definition of ''biometric identifiers.''

Vigil also raises significant questions in the context of B2B and B2C technology transactions. Among these questions is whether the standing analysis applicable to procedural violations of statutes applies equally to procedural violations of contracts. For example, B2B contracts involving personal information frequently include procedural privacy requirements, such as information security controls, storage and retention requirements and/or breach response requirements. Would a plaintiff alleging the breach of those provisions without more lack standing, just as the *Vigil* plaintiffs alleging procedural violations of BIPA lacked standing? To avoid the risk of lacking standing to bring a breach of contract claim, parties negotiating technology transactions may begin pushing for provisions that expressly link procedural or security requirements to concrete substantive interests; alternatively, they may seek an acknowledgment of that connection in the contract. Moreover, in the B2C context, *Vigil* raises the question: to what extent might courts view statutory privacy requirements as a legislature's substitute for contractual requirements when consumers lack bargaining power or a forum in which to negotiate privacy terms in consumer contracts? In other words, if private parties can negotiate and enforce procedural privacy requirements, can a legislature effectively do so via statute?

Facial-Recognition Technologies

While the case law on standing has developed, so has case law addressing facial-recognition technologies. In particular, the case law has begun to address technologies that create facial geometry templates—maps of an individual's unique facial measurements—from photographs. Social media and other companies frequently use these technologies to identify and/or group together photographs of the same person and to offer other related services associating names with faces. The main question in this case law is whether these templates are ''biometric identifiers'' within the meaning of BIPA and therefore subject to the statute's requirements.

Periodically revise policies and procedures in light of evolving case law and state statutes.

The U.S. District Court for the Northern District of Illinois recently addressed this question in *Rivera*. The plaintiffs there alleged Alphabet Inc.'s Google created face templates from photos uploaded to Google Photos to find and group together other photos of the plaintiffs. Google moved to dismiss for failure to state a claim, arguing the templates were not ''biometric identifiers'' within the meaning of BIPA because they were taken indirectly from uploaded photographs, not directly from their physical faces. The court rejected this argument, holding the statute's plain language defined a ''biometric identifier'' as ''a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry,'' and that the templates at issue fell within this definition because they were allegedly scans of face geometry.

It noted, ''a 'biometric identifier' is not the underlying medium itself or a way of taking measurements, but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person.'' *Rivera*, No. 15-cv-8211 at 12-13. Put differently, the definition of ''biometric identifier'' is technology neutral; companies creating the relevant sets of measurements cannot evade the statute by employing a different technology. The court's ruling—that such facial geometry templates qualify as ''biometric identifiers'' under BIPA—is consistent with prior cases addressing the same question in the context of similar facts. *See, e.g., Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103, 1106 (2015).

Assuming no standing hurdles, *Rivera's* approach may portend a growing tide of BIPA litigation; the number of photographs that have been similarly scanned by social media and other companies, combined with the significant damages permissible for each violation, may invite high-volume, high-stakes litigation.

Meanwhile, however, the Illinois legislature is considering an amendment that would carve out similar face templates from the definition of ''biometric identifiers.'' Other state legislatures may well monitor the Illinois General Assembly's reception of this amendment as they draft their own statues.

Practice Pointers

As BIPA case law develops and additional legislatures consider passing biometric privacy acts, companies should consider taking the following steps:

- Identify any collection, use, storage and disclosure of biometric information by the company.

- Develop policies and procedures governing the collection, use, storage and disclosure of biometric information that enable compliance with applicable law. Policies and procedures should address the following:

  - Retention, return and destruction of biometric information.

  - Physical, administrative and technical controls protecting biometric information from unauthorized use or disclosure.

  - Consumer-facing notice and consent processes.

  - Privacy Impact Assessments of systems handling biometric information.

Periodically revise policies and procedures in light of evolving case law and state statutes.

- Identify and address any gaps between the company's actual handling of biometric information and the handling as required by applicable law, policies and procedures.

- Revise agreements with vendors and any other third parties to reflect compliance obligations.