PAUL HASTINGS

Stay Current

March 2022

Follow @Paul_Hastings

Caveat Vendor: California is Considering a Biometric Information Privacy Law Modeled on Illinois' Biometric Information Privacy Act but with a Potentially Further Reach

By Adam M. Reich, Aaron Charfoos & John J. Michels

California is poised to become the latest state to enact legislation permitting a broad private right of action against private entities[1] that collect or possess biometric information. On February 17, 2022, California State Senator Robert Wieckowsi (D-Fremont) introduced Senate Bill No. 1189 for consideration. If enacted, Senate Bill No. 1189 will require any private entity in possession of "biometric information" to essentially satisfy a variation of the same requirements as Illinois' Biometric Information Privacy Act, 740 ILCS 14 et seq. ("BIPA"), by September 1, 2023. A vote is expected to be held on the bill in advance of August 31, 2022.

Senate Bill No. 1189's "Biometric Information" Differs From BIPA "Biometric Identifiers" and "Biometric Information"

Senate Bill No. 1189 and BIPA incorporate different definitions of biometric data. BIPA applies to two categories of biometric data, biometric identifiers and biometric information,[2] while Senate Bill No. 1189 contains only a singular term definition for biometric information.[3]

Under BIPA, "*biometric identifiers*" include retina scans, iris scans, fingerprints, voiceprints, and scans of hand or face geometry.[4] They expressly do not include writing samples or written signatures; photographs; human biological samples used for valid scientific testing or screening; demographic data; tattoo descriptions; physical descriptions, such as height, weight, hair color, or eye color; donated organs, tissues, or other body parts; blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federal designated organ procurement agency; biological materials regulated under Illinois' Genetic Information Privacy Act, 430 ILCS 513/1 *et seq.*; information captured from patients in health care settings or collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); or X-rays or other images or films of human anatomy used to diagnose, prognoses, or treat an illness or other medical condition or to further validate scientific testing or screening.[5] Meanwhile, "*biometric information*" under BIPA 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.[6]

In contrast, Senate Bill No. 1189 includes a broader definition of "*biometric information*" than BIPA: "a person's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that can be used or is intended to be used, singly or in combination with each other or with other identifying data, to establish individual identify."[7] The Bill further confirms that its broad definition specifically includes "imagery of" an individual's iris, retina, fingerprint, face, hand, palm, or vein patterns, or voice recordings, from which an "identifier template," including a voiceprint, can be extracted.[8] Further, Senate Bill No. 1189 purports to consider "keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information" to be "biometric information."[9]

Senate Bill No. 1189 Targets the Same Activity As BIPA But Generally In A More Restrictive Manner

Senate Bill No. 1189 targets the same activity as BIPA, namely collection, capture, purchase, receipt through trade, or otherwise obtaining biometric data, and selling, leasing, trading, profiting from, and disclosing biometric data.[10] Both Senate Bill No. 1189 and BIPA also require a private entity possessing biometric data to safeguard such data "using the reasonable standard of care" within the entity's industry, and in a manner that is the same as, or more protective than, the manner in which other confidential and sensitive information is stored by the entity.[11] However, there are four notable differences in the way Senate Bill No. 1189 approaches regulation compared to BIPA.

First, while both regulatory regimes require private entities to publish a written policy with retention schedules and permanent destruction guidelines for biometric data, Senate Bill No. 1189 specifies a more limited retention period.

Retention and Destruction Requirements	
Senate Bill No. 1189	**BIPA**
Biometric information shall be permanently destroyed on or before the earlier of: (1) the date on which the initial purpose for collecting or obtaining biometric information is satisfied, provided that the person whose biometric information was collected (a) freely consented to the original purpose for the collection; and (b) could have declined the collection without consequence; OR (2) ***one year*** after the individual's last ***intentional*** interaction with the private entity.[12]	Biometric identifiers and biometric information shall be permanently destroyed either on or before the earlier of: (1) when the initial purpose for collecting or obtaining such identifiers or information has been satisfied; OR (2) within ***three years*** of the individual's last interaction with the private entity.[13]

Second, both regulatory regimes require the private entity collecting or obtaining biometric data to provide written notice that the collection, storage, and/or use is occurring, the purpose therefor, and the length of time for which such data is being collected, stored, and/or used, and to then obtain written

release from the individual whose biometric data is affected. However, Senate Bill No. 1189 differs from BIPA in its specificity relating to the requirements for such written releases.

Written Release Requirements	
Senate Bill No. 1189	**BIPA**
The private entity must receive a written release executed by the subject of the biometric information or the subject's legal representative, but the release ***cannot be***: (1) sought through, as part of, or otherwise combined with, another consent or permission-seeking instrument or function; (2) combined with an employment contract; or (3) obtained from a minor, as opposed to his or her parent or guardian.[14]	The private entity must receive a written release executed by the subject of the biometric identifiers and biometric information, or the subject's legally authorized representative.[15] "Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment."[16]

Third, both regulatory regimes prohibit unfettered disclosure of biometric data. However, Senate Bill No. 1189 and BIPA differ in their approaches to pre-disclosure requirement.

Pre-Disclosure Requirements	
Senate Bill No. 1189	**BIPA**
No private entity shall disclose biometric information unless one of four criteria is satisfied: (1) the subject or the subject's legally authorized representative provides a written release authorizing the disclosure, ***and the release specifies that*** the data will be disclosed, the reason for disclosure, and the recipients of the biometric information; (2) the disclosure completes a financial transaction requested or authorized by the subject or the subject's legally authorized representative; (3) the disclosure is required by law; or (4) the disclosure is required by valid warrant or subpoena issued by a court of competent jurisdiction.[17]	No private entity possessing biometric identifiers or biometric information may disclose, ***redisclose, or otherwise disseminate*** such data unless one of four criteria is satisfied: (1) the subject or the subject's legally authorized representative consents; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by state or federal law or municipal ordinance; or (4) the disclosure or redisclosure is required by valid warrant or subpoena issued by a court of competent jurisdiction.[18]

Fourth, both regulatory regimes prohibit private entities from selling, leasing, trading, or otherwise profiting from biometric data,[19] but Senate Bill No. 1189 specifically clarifies that this prohibition includes use of biometric information for advertising purposes.[20]

Senate Bill No. 1189 Provides for Different Recovery Than BIPA

Senate Bill No. 1189 provides for slightly different potential recoveries than BIPA, and potentially broader reach.

Potential Recovery	
Senate Bill No. 1189	**BIPA**
Any individual alleging a violation may bring a civil action for any of the following: (1) statutory damages ranging from $100 - $1,000 per violation per day, or actual damages, whichever is greater; (2) punitive damages (3) reasonable attorneys' fees and litigation costs; and (4) any other relief, including equitable or declaratory relief, that the court deems appropriate.[21]	Any person ***aggrieved by a BIPA violation*** may recover for each violation: (1) liquidated damages of $1,000 or actual damages, whichever is greater, against a private entity that negligently violates BIPA; (2) liquidated damages of $5,000 or actual damages, whichever is greater, against a private entity that intentionally or recklessly violates BIPA; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and (4) injunctive relief and any other relief the court deems appropriate.[22]

What This All Means for Private Entities

Private entities that operate in California or interact with California residents and collect, capture, obtain, purchase, receive through trade, use, disseminate, disclose, sell, trade, and/or profit from biometric data need to be especially vigilant of the progress that Senate Bill No. 1189 makes through the California Senate this year. In the event that the bill passes and is enacted into law, this will open up a westward front for a very active plaintiffs' biometric privacy bar, and increase potential liability exposure beyond what already exists for those same private entities operating in Illinois. Moreover, the more expansive definition of "biometric information" employed under Senate Bill No. 1189, which targets behavior and images, may ensnare additional private entities in biometric privacy litigation that have otherwise been able to avoid liability under BIPA.

Given the potential enactment of Senate Bill No. 1189, it is critical that private entities that actually or potentially may collect, capture, obtain, purchase, receive through trade, use, disseminate, disclose, sell, trade, and/or profit from biometric data in California or from California residents consult with experienced counsel about best practices for updating and drafting privacy policies for public consumption, ensuring appropriate consents and notices are in place, assessing data security safeguards, and carefully evaluating the pros and cons of arbitration agreements and class action waivers.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Adam M. Reich
1.312.499.6041
adamreich@paulhastings.com

Los Angeles

Scott Carlton
1.213.683.6113
scottcarlton@paulhastings.com

Adam M. Reich
1.213.683.6190
adamreich@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

[1] Like BIPA, Senate Bill No. 1189 applies to private entities. Specifically, Senate Bill No. 1189 defines "private entity" to mean "an individual, partnership, corporation, limited liability company, association, or similar group, however organized[,]" but expressly excludes the University of California. In contrast, BIPA provides more extensive exclusions from the "private entity" definition, including state or local government agencies, Illinois courts, court clerks, and judges or justices thereof.

[2] *See* 740 ILCS 14/10.

[3] S.B. 1189, 2021-2002 Reg. Sess. (Cal. 2022).

[4] 740 ILCS 14/10.

[5] *Id.*

[6] *Id.*

[7] S.B. 1189, 2021-2002 Reg. Sess., § 1798.300(a) (Cal. 2022).

[8] *Id.*

[9] *Id.*

[10] *Compare* 740 ILCS 14/15 *with* S.B. 1189, 2021-2002 Reg. Sess., §§ 1798.301-304 (Cal. 2022).

[11] 740 ILCS 14/15(e); S.B. 1189, 2021-2002 Reg. Sess., §§ 1798.305 (Cal. 2022).

[12] S.B. 1189, 2021-2002 Reg. Sess., § 1798.301 (Cal. 2022).

[13] 740 ILCS 14/15(a).

[14] S.B. 1189, 2021-2002 Reg. Sess., § 1798.302(a)(2)(B) (Cal. 2022).

[15] 740 ILCS 14/15(b)(3).

[16] 740 ILCS 14/10.

[17] S.B. 1189, 2021-2002 Reg. Sess., § 1798.304 (Cal. 2022).

[18] 740 ILCS 14/15(d).

[19] 740 ILCS 14/15(c); S.B. 1189, 2021-2002 Reg. Sess., § 1798.303 (Cal. 2022).

[20] S.B. 1189, 2021-2002 Reg. Sess., § 1798.303 (Cal. 2022).

[21] S.B. 1189, 2021-2002 Reg. Sess., § 1798.306 (Cal. 2022).

[22] 740 ILCS 14/20.