Some members of the California legislature want their state to remain the leader for data privacy and cybersecurity regulation in the U.S. This includes protections for biometric information, similar to those under the Biometric Information Privacy Act in Illinois, 740 ILCS 14 et seq. (BIPA). State Senator Bob Wieckowski introduced SB 1189 on February 17, 2022, which would add protections for biometric information in his state on top of other statutory provisions, such as the California Privacy Rights.
If enacted, SB 1189 would significantly expand privacy and security protection for biometric information in California and likely influence additional legislative activity in the U.S. Notably, unlike some of the limitations on application in the California Consumer Privacy Act (CCPA), the Bill would apply to any private entity (defined as an individual, partnership, corporation, limited liability company, association, or similar group, however organized, other than the University of California). It could also open the door to a wave of litigation, similar to what organizations subject to the BIPA currently face.

SB 1189 includes a fairly broad definition of biometric information, tracking the definition under the CCPA that went into effect January 1, 2020:

1. “Biometric information” means 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 identity.

2. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

Many are familiar with or have encountered devices that scan fingerprints or a person’s face which may capture or create biometric information. This definition appears to go beyond those more “traditional” technologies. So, for example, if you’ve developed a unique style for tapping away at your keyboard while at work, you might be creating biometric information. The contours of this definition are quite vague, so private entities should carefully consider the capturing of certain data sets and the capabilities of new devices, systems, equipment, etc.

The Bill would prohibit private entities from collecting, capturing, purchasing, etc. a person’s biometric information unless the private entity:

- requires the biometric information either to: (i) provide a service requested or authorized by the subject of the biometric information, or (ii) satisfy another valid business purpose (as defined in the CCPA) which is included in the written public policy described below, AND

- first (i) informs the person or their legally authorized representative, in writing, of both of the biometric information being collected, stored, or used, and the specific purpose and length of time for which the biometric information is being collected, stored, or used, and (ii) receives a written release executed by the subject of the biometric information or their legally authorized representative.

In this regard, SB 1189 looks a lot like the BIPA, with some additional requirements for the written release. For example, the written release may not be combined with an employment contract or another consent form.
Under SB 1189, private entities in possession of biometric information also would be required to develop and make available to the public a written policy that establishes a retention schedule and guidelines for destroying biometric information. In general, destruction of the information would be required no later than one year after the individual’s last intentional interaction with the private entity. This is similar to the period required in the Texas biometric law.

In addition to requiring reasonable safeguards to protect biometric information, the Bill would place limitations on the disclosure of biometric information. Unless disclosed to complete a financial transaction requested by the data subject or disclosed as required by law, a written release would be required to disclose biometric information. The release would need to indicate the data to be disclosed, the reason for the disclosure, and the intended recipients.

Perhaps the most troubling provision of the Bill for private entities is section 1798.306. Again, looking a lot like the BIPA, SB 1189 would establish a private right of action permitting individuals to allege a violation of the law and bring a civil action for any of the following:

- The greater of (i) statutory damages between $100 and $1,000 per violation per day, and (ii) actual damages.
- Punitive damages.
- Reasonable attorney’s fees and litigation costs.
- Any other relief, including equitable or declaratory relief, that the court determines appropriate.

Though still early in the legislative process for SB 1189, its introduction illustrates a continued desire by state and local lawmakers to enact protections for biometric information. See, e.g., recent developments in New York, Maryland, and Oregon described in our Biometric Law Map. Before implementing technologies or systems that might involve biometric information, private entities need to carefully consider the emerging legislative landscape.

Jackson Lewis P.C. © 2022

National Law Review, Volume XII, Number 54

Source URL: https://www.natlawreview.com/article/california-state-senator-introduces-bipa-law-to-protect-biometric-information