THE BIOMETRIC BANDWAGON ROLLS ON: BIOMETRIC LEGISLATION PROPOSED ACROSS THE UNITED STATES

Date: 25 March 2019

U.S. Biometric Data Compliance & Defense Alert

By: Kenn Brotman, Erinn L. Rigney, Molly K. McGinley

The biometric bandwagon keeps rolling along as more and more states seek to regulate the collection, use, and retention of biometric data. Currently, three states, Illinois [1], Texas [2], and Washington [3], have biometric privacy laws in place, while the California Consumer Privacy Act ("CCPA") [4], which was previously covered by K&L Gates (available here), goes into effect on January 1, 2020. Now, on the heels of a seminal decision addressing the Illinois Biometric Information Privacy Act ("Illinois BIPA"), which we recently discussed (available here), Arizona, Florida, and Massachusetts have become the latest states to propose legislation addressing the issue of biometric privacy, and other states are also considering biometric privacy laws.

While the recently proposed bills all continue the growing trend of regulating the collection, retention, and use of biometric data, their approaches differ in significant respects and highlight the varying ways states are attempting to keep up with technological advances. A key difference in the approaches by the states is whether to (a) allow only the state's attorney general to enforce the biometric privacy law, or (b) create a private right of action allowing individuals, either on their own or via class actions, to seek enforcement through civil litigation seeking monetary relief, as exemplified by the hundreds of putative class action lawsuits seeking damages for violations of Illinois BIPA. Notably, the CCPA currently includes only a limited private right of action relating to "personal information," which is defined more narrowly than elsewhere in the CCPA and does not include biometric information [5].

Other distinctions include how each state defines biometric information or biometric identifier. For example, biometric information under the CCPA is defined broadly to include physiological, biological, and behavioral characteristics and includes not only the traditional fingerprint and retinal scan, but also keystroke and gait patterns as well as "sleep, health, and exercise data that contain identifying information." Washington has a similarly expansive definition, which includes "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." Illinois and Texas, on the other hand, limit the definition of "biometric identifier" to specific types of information, including fingerprints, retina or iris scans, voiceprints, or scans or records of hand or face geometry. However, Illinois BIPA applies with equal force to "biometric information," which is defined to include "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."

As more and more states consider and implement biometric privacy laws, it is becoming increasingly important for companies to ensure that they are prepared for, and complying with, the current and potentially applicable biometric privacy laws. This alert examines the biometric privacy laws most recently proposed for enactment in

Arizona, Florida, and Massachusetts and compares the approaches they take to existing statutes in other jurisdictions.

ARIZONA

On January 28, 2019, Arizona House Speaker Rusty Bowers introduced Arizona House Bill 2478 ("HB 2478"), which, if passed, will prohibit entities from capturing, converting, or storing an individual's biometric identifier in a database for a commercial purpose unless (1) it provides "a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose; or (2) advance notice [is] provided and consent [is] obtained from the individual." HB 2478 tracks the similar provisions in Washington State's biometric privacy law and exempts actions taken for security purposes such as preventing fraud or shoplifting, or protecting the security of software, accounts, or applications.

As HB 2478 prohibits the use of a biometric identifier for a commercial purpose, its scope is limited to persons that engage in the collection or retention of biometric identifiers in order to sell or disclose such identifiers for marketing purposes that are unrelated to the initial capture of an individual's biometric identifier [6]. As introduced, HB 2478 will not extend to companies utilizing biometric identifiers for employment purposes, unless the company sells or discloses such identifiers to a third party.

Similar to CCPA and Washington's law, HB 2478 broadly defines "biometric identifier" to include not only a fingerprint, retina or iris scan, or face geometry, but also any other "unique biological pattern or characteristic that is used to identify a specific individual." HB 2478 does not create a private right of action, making it more similar to the Texas and Washington State statutes and the CCPA. While actions brought by the Texas attorney general may pursue civil penalties of up to $25,000 per violation, HB 2478 makes a violation of the proposed legislation a violation of the Arizona Consumer Fraud statute [7], which provides for civil penalties of only up to $10,000 per violation [8]. It remains to be seen how courts will interpret what constitutes a "violation" for purposes of awarding damages under any of these statutes.

MASSACHUSETTS

Also in January of this year, four Massachusetts senators introduced a bill entitled "An act relative to consumer data privacy" ("S.120"). This proposed law is directed at protecting consumers and limits its reach to businesses that collect Massachusetts consumer information and meet specific revenue standards. Despite limiting its requirements to a smaller subset of companies, S.120 has a broader scope than many of the other biometric laws and mandates that businesses notify consumers about actions taken with regard to personal information, which encompasses significantly more types of consumer data. Specifically, personal information extends to any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's device."

As a subset of personal information, and similar to the Illinois and Washington statutes, biometric information also is defined broadly and includes not only retina scans, fingerprints, and handprints, but also "keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information." By

including data relating to sleep and exercise, S.120 tracks the CCPA and would extend to companies collecting information that may not be covered under other states' biometric privacy laws.

Like the CCPA, entities collecting information covered under S.120 will be required to provide consumers advance notice about the different categories of personal information being collected, the business purpose for such collection, and any potential disclosure to third parties. In addition to the notice requirements, S.120 allows consumers to obtain a copy of their personal information that was collected and request deletion of all such information. If passed, companies will have an affirmative obligation to display on their websites information similar to the content of the consumer notice. S.120 also includes a non-discrimination provision that prohibits businesses from treating consumers differently who exercise their rights to request or delete information or opt out of third party disclosure.

Various exemptions exist within S.120, most notably for businesses collecting personal information of their employees so long as it is within the scope of employment. What is markedly absent from the proposed statute is any specific requirement pertaining to the storage of consumer biometric information. Perhaps anticipating the litigation on the issue of actual injury and standing that has occurred with respect to Illinois BIPA, S.120 provides for a private right of action, which closely mimics the "no harm" requirement as recently interpreted by the Illinois Supreme Court. As drafted, S.120 provides that a violation "shall constitute an injury in fact to the consumer who has suffered the violation, and the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this chapter."

FLORIDA

In late February 2019, Florida also jumped on the biometric bandwagon when the "Florida Biometric Information Privacy Act" was introduced in both the House and Senate. Florida's proposed laws closely track Illinois BIPA, regulating private companies' collection, storage, and dissemination of individuals' biometric information. As under Illinois BIPA, "biometric identifier" includes retina or iris scan, fingerprint, voice print, or scan of hand or face geometry," while "biometric information" includes any information, regardless of the manner in which it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."

Under the Florida Biometric Information Privacy Act, any entity that possesses biometric information will be required to develop and implement a publicly available, written policy addressing its procedures for the storage and destruction of biometric information. Advance notice to individuals along with written authorization is required by Florida's proposed laws before any company may collect, capture, purchase, or otherwise obtain a person's biometric information. Both bills again mirror the Illinois statute by prohibiting the sale, lease, trade, or profit from an individual's biometric information and require advance authorization prior to disclosure to third parties.

As introduced, the proposed laws provide for a private right of action, which is framed in terms identical to Illinois BIPA, and allows "any person aggrieved by a violation" to proceed in court. Also similar to Illinois BIPA, the proposed laws call for the imposition of liquidated damages in the amount of $1,000 for negligent violations, $5,000 for intentional or reckless violations, or actual damages if greater, plus reasonable attorney fees. If passed, the new Florida law could take effect as early as October 2019.

CONCLUSION

Though the fate of these proposed statutes as well as other pending legislation is unclear, companies that may be collecting, storing, or using biometric information should continue to monitor state law developments to ensure compliance with the law. In light of the clear trend of states jumping on the biometric bandwagon, and the speed with which some of the new laws are being proposed, companies may also be well-served by drafting and implementing policies and procedures to protect biometric information that are compliant with existing and anticipated state statutes, as potentially applicable.

NOTES:

[1] 740 ILCS 14/5.

[2] TEX. BUS & COM. § 503.001.

[3] WASH. REV. CODE § 19.35.

[4] CAL. CIV. CODE § 1798.100 *et seq*.

[5] CAL. CIV. CODE § 1798.150, limiting private right of action to personal information as defined in as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5.

[6] Of the current biometric privacy laws in place, only Illinois BIPA requires notice and consent for the capture of a biometric identifier, regardless of the purpose, while Washington State, Texas, and HB 2478 require notice and consent only if the identifier is to be used for a commercial purpose.

[7] ARIZ. REV. STAT. § 44-1530.

[8] ARIZ. REV. STAT. § 44-1531.

