BUSINESS INFORMATION GROUP

white paper

BIOMETRIC DATA PRIVACY LAWS AND FINGERPRINTING

With the use of biometric data on the rise, familiarization with state laws is critical in developing and implementing internal policies and procedures.

As the use of biometric data expands and becomes increasingly ubiquitous in everyday life, more states are seeking to protect consumers by regulating the collection, use, and retention of biometric data. Currently, Illinois, Texas, and Washington have biometric privacy laws in place and California will as well when its California Consumer Privacy Act ("CCPA") goes into effect on January 1, 2020. Many additional states are proposing similar legislation including Arizona, Florida, and Massachusetts.[1]

With more states following the trend of enacting biometric privacy laws, organizations should consider implementing policies and procedures that align with existing state biometric privacy laws as a measure of good practice.

WHAT IS BIOMETRIC DATA?

A "biometric identifier" is generally defined as measurable physical and behavioral characteristics that enable the establishment and verification of an individual's identity.[2] Some states have broad definitions of "biometric identifier" that encapsulate more biological characteristics however; all states with legislation or proposed legislation consider fingerprints to be protected biometric information.[3]

BACKGROUND

Illinois became the first state in 2008 to pass a law regarding the collection of biometric data. The Illinois Biometric Privacy Act (BIPA) imposes requirements on businesses that collect or obtain biometric information.[4]

[1] States with legislation proposed include Massachusetts, New York , Delaware, Alaska, Arizona, and Michigan www.winston.com/en/privacy-law-corner/several-states-considering-laws-regulating-the-collection-of-biometric-data.html

[2] https://www.biometricupdate.com/201601/what-are-biometrics-2

[3] California has a broad definition that includes physiological, biological, and behavioral characteristics that includes fingerprints, retinal scans, keyboard strokes, gait patterns, sleep, health, and exercise data. Washington has a similarly expansive definition. Illinois and Texas limit the definition to finger prints retina or iris scans, voiceprints, or scans or records of hand or face geometry. www.natlawreview.com/print/article/biometric-bandwagon-rolls-legislation-proposed-across-the-united-states

[4] 740 ILCS 14

Illinois requires a business to

1. Inform the consumer *in writing* that biometric information is being collected and stored;
2. Inform the consumer *in writing* of the purpose and length of time the information will be stored and used; and
3. Secure *written* consent from the consumer.

Texas and Washington have similar requirements for a business to

1. Inform the consumer that biometric information is being collected and stored;
2. Inform the consumer of the purpose for the collection of biometric information; and
3. Secure consent from the consumer.[5][6]

California will require businesses to

1. Inform the consumer that biometric information is being collected and stored;
2. Inform the consumer of the purpose for the collection of biometric information;
3. Secure consent from the consumer;
4. Disclose all information that will be and has been collected; and
5. Provide the right to consumers to access and delete stored biometric information.[7]

Illinois, Texas, and Washington require that businesses store, transmit, and protect data from disclosure with reasonable care in addition to maintaining a publicly available written policy identifying retention rules. Other states with proposed legislation closely track the Illinois, Texas, and Washington acts. Massachusetts's proposed law requires organizations to give consumers; advance notice, disclose the purpose for the collection, respond to opt-out requests, and provide the right to consumers to access and delete biometric information.[8] New York, Alaska, Michigan, and Delaware's proposed laws are similar to BIPA.

ENFORCEMENT OF BIOMETRIC PRIVACY LAWS AND PENALTIES

One way biometric protection law differs among states is whether

a. Only the states attorney general can enforce the biometric privacy law; or
b. There is a private right of action that allows individuals, on their own or as part of a class action, to seek enforcement of the law through civil litigation.

Illinois allows a private right of action for individuals. In addition to attorney and litigation expenses, individuals can be awarded the greater of actual damages, or $1,000 in liquidated damages for negligent violations or $5,000 in liquidated damages for intentional or reckless violations.

Texas and Washington require that the attorney general bring action to recover a civil penalty. Texas allows recovery of a civil penalty of not more than $25,000 for each violation.

California's CCPA requires that the attorney general bring action. Proposed legislation in other states varies dependent on whether the attorney general or an individual is permitted to file suit.

[5] TEX. BUS & COM. §503.001

[6] WASH. REV. CODE §19.375

[7] CA CIVIL §1798, effective Jan.1, 2020.

[8] *Supra*, Note 1

RECENT LITIGATION

In a recent class action in Illinois, Rosenbach v. Six Flags Entertainment Corp, the Plaintiff alleged Six Flags violated BIPA when the company failed to inform the Plaintiff that a fingerprint was required in order to be issued a season pass.[9] The Plaintiff did not allege that these violations caused any harm financially or otherwise. The Illinois Supreme Court held that private individuals may bring suit under BIPA when the harm results in a violation or denial of a person's legal rights.[10] Courts have differed on what types of injuries constitute a violation but many are finding guidance from the Illinois case.

CONCLUSION

With the speed at which new legislation is being proposed, companies that collect and use fingerprint data should implement procedures and policies that conform to established state laws. Most state laws require that a business notifies the consumer that biometric information is being collected, states the purpose of the collection, and secures an affirmative consent from the consumer. As a measure of best practice in obtaining biometric information, entities should provide advance notice and secure informed written consent from the consumer. To the extent applicable, Fieldprint implements procedures to comply with these laws.

[9] Rosenbach v. Six Flags Entertainment Corp., No. 123186, 2019 WL 323902 (IL Jan. 25,2019)

[10] Id., *BIPA allows any aggrieved individual to bring suit. The court held that aggrieved meant anyone whose rights under BIPA were violated.* www.skadden.com/insights/publications/2019/01/illinois-supreme-court