Washington becomes the third state with a biometric privacy law: five key differences

Data Protection, Privacy and Security Alert

21 JUN 2017
By: Jim Halpert

The State of Washington has become the third state (after Illinois and Texas) to enact a law regulating biometric information (HB 1493).

The new law, enacted in mid-May, goes into effect on July 23, 2017.

Although the Washington law has consumer protection goals similar to those that motivated the Illinois Biometric Information Privacy Act (BIPA) (740 ILCS 14/) and the Texas biometric law (Tex. Bus. & Com. Code Ann. § 503.001), HB 1493 is more narrowly tailored. The new Washington law reflects a more nuanced view of biometric data: that it can be inadvertently collected in situations that should not require consent, that it can be used for some beneficial purposes (eg, fraud prevention) that do not require consent and that “biometric data” should be defined with precision to avoid covering information that is not broadly understood to be biometric.

The law differs from the Illinois and Texas first-generation laws in five important ways:

1. **HB 1493 focuses on "enrollment" of biometric identifiers**

The scope of Washington's new law differs principally from both BIPA and the Texas biometric law by limiting "enrolling" biometric identifiers in a database for commercial purposes and further sale or disclosure of those
enrolled identifiers – instead of broadly requiring affirmative consent for virtually any collection, use or disclosure of biometric data. Under the Washington law, biometric identifiers may be collected without consent but may not be "convert[ed] it into a reference template that cannot be reconstructed into the original output image, and store[d] in a database that matches the biometric identifier to a specific individual" unless consent has been obtained.

In order lawfully to enroll a biometric identifier in a database for a commercial purpose, a person must (i) provide notice; (ii) obtain consent; or (iii) provide a mechanism to prevent subsequent use of the biometric identifier for a commercial purpose. Only after a biometric identifier has been enrolled in a database for commercial purposes does HB 1493 prohibit selling, leasing or disclosing it without individual consent.

2. The definition of biometric identifier does not include photographs, video or audio recordings or face geometry

The definition of "biometric identifier" under HB 1493 specifically excludes physical and digital photographs and video and audio recordings. The Washington law instead defines "biometric identifier" in clear terms as "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." The definition excludes "physical or digital photograph, video or audio recording or data generated therefrom." It also does not mention "face geometry" in its biometric identifier definition.

The explicit exclusion of photographs, and absence of a reference to face geometry, is in response to lawsuits against companies alleging violations of the Illinois BIPA for collecting and using information about faces derived from photographs without user consent. Such lawsuits have plagued companies like Google, Shutterfly and others whose services involve allowing users to group their photographs by automatically recognizing faces. For example, in a case against Shutterfly, the plaintiff, Brian Norberg, claimed that a Shutterfly user uploaded at least one photo of the plaintiff to Shutterfly in the course of creating a wedding invitation. Upon uploading the photo, the plaintiff said that Shutterly automatically scanned and analyzed his face, extracted his biometric identifiers and used those identifiers to create a template of his face. The plaintiff further alleged that Shutterfly then prompted the user who uploaded the photos to "tag" his face, at which point the user tagged the face in the photo as that of "Brian Norberg."

3. The notice and consent requirements are more flexible

The Washington statute does not prescribe the kind of notice that needs to be provided or consent obtained prior to enrolling a biometric identifier. Instead, it says that "[t]he exact notice and type of consent" required for enrollment is "context-dependent" and that notice need only be provided in a way that is "reasonably designed to be readily available to affected individuals."

This is in contrast with BIPA, which requires that written notice be provided and that written release be obtained prior to collecting a biometric identifier or biometric information. HB 1493 is similar to the Texas law in not specifying how individuals need to be informed or consent obtained, and goes one step further than Texas by stating that the notice and consent methods may be context-dependent – a standard consistent with the statements regarding privacy good practices issued in the Obama Administration in its report on Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy and the FTC’s 2012 report on Protecting Consumer Privacy in an Era of Rapid Change.

4. HB 1493 includes a number of important exceptions to the notice and consent requirement

Of the three biometric laws, the new Washington law is the only one that exempts use of a biometric identifier for purposes of security or fraud prevention. Unlike both BIPA and the Texas biometric law, HB 1493 broadly exempts the collective, capture, or enrollment of a biometric identifier from the notice and consent requirement in furtherance of a "security purpose." Security purposes include preventing shoplifting, other misappropriation or theft, and other purposes in furtherance of protecting security.

In addition, the law exempts use of biometric identifiers in ways that conflict with the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act as well as use by law enforcement. It also does not require consent prior to selling, leasing or disclosing enrolled biometric identifiers if the sale, lease or disclosure is (i) consistent with the requirements of the biometric law; (ii) necessary to provide a product or service subscribed to,
requested by or expressly authorized by the individual; (iii) necessary to effect, administer, enforce or complete a financial transaction requested, initiated or authorized by the individual and where the recipient maintains confidentiality of the biometric identifier and does not further disclose it; (iv) required or expressly authorized by a federal or state statute or court order; (v) made to a third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the law; or (vi) made to prepare for litigation or to respond to or participate in judicial process.

5. There is no private right of action

Only the Washington Attorney General may enforce the law’s requirements. As mentioned above, a number of class action lawsuits have been filed against companies under BIPA. Unlike BIPA – but like the Texas biometric law – the Washington law does not create a private right of action.

Similarities to existing state laws

HB 1493 is similar to both BIPA and the Texas biometric privacy law in that it contains data security and retention requirements for safeguarding biometric information. The new law will require that persons who knowingly possesses a biometric identifier that has been enrolled for a commercial purpose (i) take reasonable care to guard against unauthorized access to and acquisition of biometric identifiers; and (ii) retain biometric identifiers for no longer than necessary to comply with the law, protect against fraud, criminal activity, security threats or liability or to provide services for which the biometric identifier was enrolled.

DLA Piper lawyers were involved in drafting HB 1493 and actively monitor state biometric privacy legislation. If you have questions about this law, the Illinois or Texas laws, or state legislative activity in this area, feel free to contact the authors.

AUTHORS

Jim Halpert
Partner
Washington, DC | T: +1 202 799 4000
[Email protected]