THE
NATIONAL LAW REVIEW

Washington Enacts a Biometric Privacy Statute in a Departure from the Existing Standard

Tuesday, June 13, 2017

Article By
Privacy and Data Security
Proskauer Rose LLP
New Media and Technology Law Blog
Communications, Media & Internet
Washington

We have been writing about the biometric privacy legal landscape, which has thus far been dominated by the Illinois Biometric Information Privacy Act (BIPA). While there are a number of states that are considering bills modeled after BIPA, Washington has enacted a bill that takes a dramatically different approach. On May 16, 2017, HB 1493 (the "Washington Statute," or the "Statute") was signed into law by Governor Jay Inslee and will become effective on July 23, 2017.

The stated purpose of the Statute is to require a business that collects and can attribute biometric data to a specific individual to disclose how it uses that biometric data and provide notice to and obtain consent from an individual before enrolling or changing the use of that individual's biometric identifiers in a database. Unlike BIPA, the Statute does not provide a private cause of action; it may be enforced solely by the state attorney general under the Washington consumer protection act. It should be noted, however, that Washington has traditionally been one of the leading states with regard to the enforcement of consumer privacy.

As we have seen in other biometric privacy legislation, the Washington Statute has notice and consent requirements for the enrollment of a "biometric identifier" in a database for a commercial purpose. Under the Statute, a person may not "enroll biometrics in a database for a commercial purpose without first providing notice, obtaining consent, **or** providing a mechanism to prevent the subsequent use of the biometrics for a commercial purpose." [emphasis added]. Interestingly, the bill as originally drafted required both notice and consent, but the Statute as now in effect requires either notice, consent, or a mechanism to prevent the subsequent use of the biometrics for a commercial purpose.

Unlike BIPA and the laws that have followed it, the Washington Statute draws a distinction between the "enrollment" of biometric data and the mere "capture" or "collection" of such information. "Enroll" in the Statute means to collect a biometric identifier of an individual, convert it into a reference template, and store it in the biometric system's database for later comparison and matching to an individual. Biometric samples converted in a reference template format "cannot be reconstructed into the original output image." If an entity does not enroll biometric information for a commercial purpose in the precise way described in this definition – collection, conversion into a reference template, and storage in a database – the entity is not subject to the Statute's requirements.

At this juncture, it is unclear what the implications would be for an entity that collects biometric information but does fully "enroll" such information. During debate of the bill, statewide business associations stressed that restrictions should focus on the use, but not the collection, of biometric information, particularly when such data specifically identifies an individual. It is not apparent what the purpose of that distinction might be, though it seems that the drafters took the distinction into account, at least in part, when defining the term "enrolled." which requires more than the mere collection of biometric identifiers.

Additionally, the limitations on disclosure and retention do not apply to biometric identifiers that have been "unenrolled," that is, not captured and converted into a digitized template and stored in a database that matches the biometric identifier to a specific individual. While a complete interpretation of this may require guidance from the Washington Attorney General or a court, the term "unenrolled" suggests removal of biometric

template data linked to a specific individual from a database, perhaps a reference to anonymous, de-identified biometric data. This suggests that the Washington legislature is most concerned with protecting its citizens from unknowingly having their biometric information stored in a database (and capable of being used commercially as a personal identifier) rather than a one-time collection and use.

Under the Statute, notice is deemed sufficient as a disclosure that is given through a "procedure reasonably designed to be readily available to affected individuals," and the Statute recognizes that the exact wording and style of notice is "context-dependent," particularly given that biometric collection could happen in a brick-and-mortar environment, online or on mobile devices. Echoing many states' requirements to protect consumers' personal information with reasonable security, the Statute requires that the holder of biometric data enrolled for commercial purposes must "guard against unauthorized access to and acquisition of the biometric identifiers" and may retain biometric data no longer than is reasonably necessary to, among other things, provide the services for which the biometrics were enrolled. Once a business enrolls biometric identifiers for a commercial purpose, the Statute prohibits entities from using or disclosing biometric identifiers in a manner that is inconsistent with the terms under which the data was originally provided "without obtaining consent for the new terms of use or disclosure."

Similar to BIPA, the Washington Statute places limitations against the sale or disclosure of biometric data to third parties. Absent individual consent, under the Statute, a person may not sell, lease, or otherwise disclose the biometrics to another person for a commercial purpose unless, among other things:

- a person provides notice or a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose, guards against unauthorized access, and retains the data for no longer than is reasonably necessary based on the context;
- it is necessary to provide a product or service expressly authorized by the individual;
- it is necessary to effect a financial transaction that the individual requested, initiated, or authorized and the third party to whom the biometrics are disclosed maintains confidentiality of the biometrics;
- it is required or expressly authorized by a federal or state statute, or court order;
- it is made to a third party who contractually promises to not further disclose the biometric identifier and not enroll the biometric identifier in a database for commercial purposes inconsistent with the requisite statutory restrictions; or
- it is made to prepare for litigation or to respond to or participate in judicial process.

If any one of the listed actions above is shown, consent need not be obtained prior to selling, leasing, or disclosing biometrics to a third party. Given the number of exceptions, this begs the question: in what scenario is an individual protected from having her biometric information sold or disclosed to a third party?

The Statute defines "biometric identifiers" as data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. Under the text, "biometric identifier" does not include "a physical or digital photograph, video or audio recording or data generated therefrom…." Depending on the interpretation of such exclusion, it is uncertain whether the Statute applies to photo tagging activities from social media and photo storage apps that use facial recognition technology to develop faceprints from user uploaded photos, a practice that has been the subject of much litigation with respect to BIPA. It could be argued that the Statute expressly exempts facial recognition scanning of digital photographs; on the other hand, some might contend that even if the Statute exempts digital photographs from its reach, the scanning of such photographs using facial recognition technology to make facial templates would be regulated under the Statute.

The Statute's notice and consent requirements for enrolling a biometric identifier in a database are curtailed by several additional carveouts. As discussed above, the limitations on disclosure and retention do not apply to biometric identifiers that have been "unenrolled." The Statute also provides that notice and consent requirements are not applicable if an entity collects or enrolls a biometric identifier and stores it in a biometric system "in furtherance of a security purpose." "Security purpose" is defined broadly as "the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person." It remains to be seen how broadly "security purpose" will be construed, and whether it would cover, for example, a mobile platform storing fingerprints to secure a phone, a payment card brand partnering with e-commerce retailers to authenticate transactions using emerging data security features that use biometrics in lieu of, or in addition to, passwords.

Companies that offer online or mobile services that involve the collection of covered biometric information should examine the Washington Statute closely (as well as the other proposed biometric privacy legislation being debated in other statehouses). Covered entities that fall under the Washington statute may have to consider changes to their notice and consent practices (some of which may be different than what is required under Illinois' BIPA), or choose to avoid collection of biometric data at all, except as per the exceptions enunciated

under the Statute. To the extent a company is already collecting biometric information, it should now be aware of the Washington Statute.

This post was written by Divya Taneja.

Source URL: https://www.natlawreview.com/article/washington-enacts-biometric-privacy-statute-departure-existing-standard