

Wash. Expands Biometric Privacy Quilt With More Limited Law

By **Allison Grande**

Law360, New York (July 21, 2017, 7:15 PM EDT) -- A newly enacted Washington state law governing the collection and use of consumers' biometric information is seen as a more business-friendly alternative to an Illinois law that has provoked a flurry of consumer suits, and may stand as a model for states to emulate in future legislation, experts say.

Like the Illinois 2008 law, and one enacted by Texas in 2009, Washington's new law — the third such state law nationwide — requires businesses that collect biometric data such as fingerprints, voiceprints and retina scans to disclose how it would be used and provide notice to and obtain consent from the owner before using it.

But Washington deviates sharply from Illinois by omitting hotly contested provisions that businesses argue expose them to heightened legal liability, notably the right of consumers to sue and for companies to be held accountable for the collection and handling of digital photographs and audio recordings.

"If you look at all the exclusions in the Washington bill, it doesn't appear to be anywhere close to providing consumers with the type of privacy protections that the Illinois one does and seems to be a much more industry-friendly piece of legislation," said Bradley S. Shear, managing partner of Shear Law LLC. "If I'm representing a company, I'd say let's try to focus on the Washington state law because it provides us [with] greater flexibility, and let's hope that bill becomes the standard across the country."

The Texas statute hasn't attracted as much attention, in part because it doesn't grant consumers a private right to sue. Illinois residents' ability to sue on claims of unlawful collection of biometric data, and win between \$1,000 and \$5,000 in damages per violation, has spurred a wave of lawsuits against major companies including Facebook, Google, Snapchat and Shutterfly.

"What makes the Washington law interesting — and what should make it an example for states to consider going forward — is that it specifically avoids many of the problems that plague Illinois' Biometric Information Privacy Act," Benesch Friedlander Coplan & Aronoff LLP partner David Almeida said.

In another sharp departure from the Illinois bill, only the Washington state attorney general has authority to enforce the biometrics law, legal experts said.

"We've seen that the Illinois statute has created quite a bit of private litigation, whereas thus far we are not aware of any enforcement by the Texas attorney general," BakerHostetler partner Melinda McLellan

said, referring to the fact that the Texas legislature also made it impossible for consumers to sue. "The Washington AG may choose to be more active in this space, but the lack of a private right of action likely will keep the plaintiffs' bar away."

In seeking redress under the Illinois law, consumers have largely honed in on the collection of information from photographs or scans that identify their facial features. Google is currently pressing for the Seventh Circuit to review a recent Illinois federal court's refusal to dismiss a putative class action accusing it of unlawfully scanning photos to create detailed face templates.

Google argues that the question of whether the statute applies to information derived from photographs warrants immediate review, while Facebook is fighting a similar action that has been allowed to remain in California court over the legality of the site's facial-recognition and tagging features.

Snapchat has also been sued under the Illinois law for collecting facial templates through its "Lenses" feature in a suit that was voluntarily dropped last year, and the maker of the National Basketball Association 2K video game series has urged the Second Circuit to uphold a lower court's dismissal of a proposed class action accusing it of collecting and retaining gamers' facial scans.

"If you're on the privacy or consumer protection side, that's what you want, a private right of action, so you can assert your rights and have a way to see things through instead of being at the mercy of state attorneys general to enforce the law," Shear said.

Aside from blocking consumers from suing for violations, the Washington state law also appears to provide a boost to businesses by excluding the types of information and the methods of data collection that have spurred the brunt of the litigation under the Illinois bill, attorneys noted.

The newly enacted Washington law defines "biometric identifier" 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 explicitly excludes "a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used or stored for health care treatment, payment or operations under the federal Health Insurance Portability and Accountability Act."

Washington's new biometric law "is more sensible and targeted than some other biometric laws because it applies only to biometric identifiers stored in a database that matches those identifiers to specific individuals," Covington & Burling LLP data privacy and cybersecurity chair Kurt Wimmer said. "Helpfully, it explicitly excludes digital photographs and information gathered from digital images."

The Washington state law also gives companies more leeway to use biometric data for noncommercial purposes, according to attorneys. While the Texas and Illinois law require opt-in consent in basically all circumstances for the collection, use and disclosure of biometric information, the Washington law frees from these requirements information that is gathered to carry out a financial transaction that an individual has requested or is used to protect against or prevent actual or potential fraud.

"It appears that Washington is trying to have the best of all worlds, by protecting citizens from the sale and commercialization of biometric databases while at the same time not restricting businesses that are using the data for purposes such as enhancing security, which is becoming increasingly common due to the rise of two-factor authentication," Sharon Klein, who chairs Pepper Hamilton LLP's privacy, security

and data protection practice, said.

In another departure from its predecessors, the Washington law focuses on businesses that "enroll" these biometric identifiers for a commercial purpose into a database that matches it to a specific individual, while the Illinois and Texas laws center on the isolated capture and possession of individual pieces of biometric data.

"There's been a bunch of real uncertainty around the Illinois and Texas laws, which were passed before there was much use of information that came close to being biometric data," said Jim Halpert, co-chair of DLA Piper's global data protection, privacy and security practice. "The Washington state law is what I would call a second-generation, more nuanced approach."

With its more narrow focus, the Washington state bill is likely to allow for the emerging biometrics industry to continue to grow and innovate while enabling the attorney general to clamp down on the most egregious violations, a path that is likely to appeal to the 47 states without biometric privacy regulation on the books, attorneys say.

"As the computing power of mobile devices becomes increasingly strong and the ability to do real-time facial recognition and other types of scanning becomes more prevalent, there will likely be more regulation around this issue," Tyler Newby, the co-chair of Fenwick & West LLP's privacy and information security group, said. "While the form which that takes still remains to be seen, there are many applications of biometric scanning that could be beneficial to consumers, and it would be important that legislation not chill those developments."

Lawmakers in Alaska, Montana and New Hampshire are weighing bills that are similar in scope to the Illinois legislation and allow for private suits against companies accused of violating the statutes. Connecticut, on the other hand, is considering narrower legislation that focuses only on the use of facial recognition for marketing purposes.

Given the push in recent years to narrow the Illinois legislation through proposed amendments such as limiting liability to data collected directly from a user rather than information garnered from a previously taken photo, attorneys expect that while Illinois will remain the high bar for companies to contend with, it's unlikely to be replicated around the country.

"While we expect the current rash of class actions under the Illinois BIPA to continue until in the near future, we expect that states considering similar laws going forward will follow Washington's example and enact more common-sense legislation in this important area," Almeida said.

--Editing by Pamela Wilkinson and Philip Shea.