Bloomberg Law

Privacy Law Watch™

Legislation

Washington's New Biometric Privacy Statute and How It Compares to Illinois and Texas Law

Biometric Privacy

As state biometric privacy laws have grown in number, so has biometric privacy litigation, making it imperative that businesses operating across the U.S. understand each state's requirements and how they overlap and differ from those of other states, the author writes.

BY LARA TUMEH

Washington recently became the third state to pass a statute regulating the commercial use of biometric identifiers. The growing trend of state biometric privacy legislation began in 2008, when Illinois enacted the Biometric Information Privacy Act (BIPA). Shortly afterwards, Texas passed a similar statute. Since then, Alaska, Connecticut, Montana, and New Hampshire have considered enacting their own biometric privacy bills.

As state biometric privacy laws have grown in number, so has biometric privacy litigation. Given this backdrop, businesses operating across the U.S. will need to understand each state's requirements and how they overlap and differ from those of other states. And on that note—a look into Washington.

What Is a Biometric Identifier? Washington's statute defines a ''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 expressly 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 of 1996.'' Engrossed Substitute House Bill 1493 (signed May 16, 2017) § 3(1).

Lara Tumeh is a technology and privacy associate at Alston & Bird LLP in Atlanta.

Washington's definition of a biometric identifier is different from those of Illinois and Texas in one significant respect. Illinois's and Texas's definitions expressly include a record of ''hand or face geometry.'' *See* 740 ILCS 14/10; Tex. Bus. & Com. Code Ann. § 503.001(a). Washington's statute does not.

The Illinois statute's inclusion of ''a scan of hand or face geometry'' generated a flurry of class action litigation starting in 2015. Social media and other companies frequently use technologies that create facial geometry templates—maps of an individual's unique facial measurements—from photographs. Companies use these technologies to identify and/or group together photographs of the same person—associations they then use for internal purposes and/or for customer offerings. Over the past few years, plaintiffs have brought actions against large social media companies, alleging that their facial templates were biometric identifiers subject to Illinois's statute and that the companies' handling of those templates violated the statute.

Washington's decision not to expressly include records of ''hand or face geometry'' in its definition of a biometric identifier is significant against this backdrop. Also significant is Washington's decision to expressly exclude ''physical or digital photographs'' from the definition of a biometric identifier. On the one hand, these decisions could lead courts to conclude that facial geometry templates derived from photographs are not biometric identifiers within the meaning of the statute. On the other hand, courts could come to the opposite conclusion; although the statute excludes a ''video or

 ISSN 0000-0000

audio recording *or data generated therefrom*'' from the definition of a biometric identifier, it does not add ''or data generated therefrom'' to its exclusion of physical or digital photography from the definition of a biometric identifier. The extent to which Washington regulates facial geometry templates therefore remains unclear—a key risk consideration for businesses using facial recognition technologies in that state.

Finally, Washington's definition of a biometric identifier implicates call centers and other businesses that may use voiceprints. But how exactly is unclear. On the one hand, the statute expressly includes a ''voiceprint'' in the definition of a biometric identifier. On the other hand, the definition expressly excludes a ''video or audio recording or data generated therefrom.'' § 3(1). In reality, some voiceprints may actually be data generated from audio recordings. The status of such voiceprints under the statute is unclear. Companies using them will need to account for the legal risk generated by this tension in the statute.

Comparative Chart
Illinois, Texas, and Washington Biometric Privacy Statutes

	Illinois 740 ILCS 14	Texas Tex. Bus. & Com. Code Ann. § 503.001	Washington Engrossed Substitute House Bill 1493 (signed May 16, 2017)
Is the scope of the statute limited to a commercial purpose?	No	Yes. A commercial purpose may include a security purpose.	Yes. A commercial purpose may not include a security purpose.
Notice and consent requirements	Both notice and consent must be in writing. Notice must state (1) the fact that a biometric identifier or biometric information is being collected or stored, and (2) the specific purpose and length of term for which it is being collected, stored, and used.	Notice must precede the capture of the biometric identifier.	The exact notice and type of consent required is "context-dependent." Notice must be "given through a procedure reasonably designed to be readily available to affected individuals." A new use or disclosure requires new consent.
Retention requirements	Retention is permitted until "the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." Retention schedule must be publicly posted.	Destruction is required "within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires," absent enumerated exceptions.	A business may retain a biometric identifier "no longer than is reasonably necessary" to (1) comply with law or a court order, (2) protect against fraud, criminal activity, claims, security threats, or liability, and (3) provide the services for which the biometric identifier was enrolled.
Does the statute create a private right of action?	Yes	No	No
What damages are authorized?	Negligent violations: the greater of $1,000 or actual damages. Intentional or reckless violations: the greater of $5,000 or actual damages. (Statute also provides for attorney's fees.)	Maximum of $25,000 per violation.	Maximum of $500,000.
Is the sale of biometric identifiers permitted?	No	Yes, under enumerated circumstances (see chart below).	Yes, under enumerated circumstance (see chart below).
Is disclosure of biometric identifiers permitted?	Yes, under enumerated circumstances (see chart below).	Yes, under enumerated circumstances (see chart below).	Yes, under enumerated circumstances (see chart below).

Source: Lara Tumeh — Bloomberg BNA

Comparison Chart

Commercial Purpose Limitation Washington's regulation of biometric identifiers is limited in substantive scope; the statute governs the collection, retention, use, and disclosure of biometric identifiers for a ''commercial purpose'' only. The statute defines a ''commercial purpose'' as ''a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier.'' A ''commercial purpose'' expressly excludes a ''security purpose''—that is, ''preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value.'' § 3.

This definition of ''commercial purpose'' limits the scope of Washington's statute in several significant respects. First, the definition appears to leave a business's internal use of biometric identifiers unregulated; the statute applies only to the sale or disclosure of biometric identifiers ''to a third party''—language added by a later draft of the bill. The statute also applies to use of biometric identifiers only for a specific subset of ''marketing'' purposes—marketing unrelated to the initial transaction involving the collection of the biometric identifier.

This commercial purpose limitation distinguishes Washington's statute from those of Illinois and Texas. The Illinois statute includes no parallel commercial purpose limitation. And unlike Washington's statute, which expressly excludes collection or use for a ''security purpose'' from its scope, the Illinois statute expressly highlights the need for a biometric privacy act based on the increased use of biometrics in ''security screenings.'' 740 ILCS 14/5(a). The Washington statute's commercial purpose limitation also distinguishes it from Texas's statute; although both states' statutes are limited to collection and use for a ''commercial purpose,'' Texas law does not define that term—creating uncertainty for businesses handling biometrics in that state.

Notice and Consent Requirements: the Clear and the Confusing Washington requires notice and consent in certain circumstances relating to biometric identifiers. Specifically, it provides that no person may enroll a biometric identifier in a database for a commercial purpose ''without first [1] providing notice, [2] obtaining consent, **or** [3] providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose.'' § 2.

Like Texas, Washington creates no specific substantive requirements for notice or consent. Washington provides only that ''the exact notice and type of consent required . . . is context-dependent,'' *id.* § 19.001.001(2)—an approach consistent with the Federal Trade Commission's 2012 report on Protecting Consumer Privacy in an Era of Rapid Change. Illinois, in contrast, does create substantive notice requirements. Notice must state (1) ''that a biometric identifier or biometric information is being collected or stored'' and (2) ''the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used.'' 740 ILCS 14/15(b).

Also like Texas, Washington creates no specific procedural requirements for providing notice or consent. Washington provides only that notice must be ''given through a procedure reasonably designed to be readily available to affected individuals.'' § 2(2). Illinois, in contrast, requires that both notice and consent be in writing.

Finally, Washington includes a unique provision prohibiting use or disclosure of a biometric identifier ''in a manner that is materially inconsistent with the terms under which the biometric identifier was originally provided, without obtaining consent.'' § 2(5).

Reasonable Security Measures All three statutes require a business to enact ''reasonable'' security measures to protect biometric identifiers. Unlike Illinois and Texas, Washington's reasonable security requirement applies only to businesses that ''knowingly'' possess biometric identifiers.

Restrictions on the Disclosure and Sale of Biometric Identifiers All three statutes also prohibit the disclosure of biometric identifiers, except in specific enumerated circumstances. Of the three states, Washington

  PRA ISSN 0000-0000

creates the broadest set of exceptions to the general bar against disclosure.

All three states generally allow disclosure:

- if the individual has consented;
- if disclosure is required under other law;
- if disclosure is in response to a warrant (Ill., Texas), court order (Wash.), or subpoena (Ill.); and
- if disclosure is necessary to complete a financial transaction authorized by the individual.

As to the third of these circumstances, Washington uniquely provides the additional caveat that ''the third party to whom the biometric identifier is disclosed'' must also ''maintain[] confidentiality'' and ''not further disclose the biometric identifier except as otherwise permitted'' by the statute. § 2(3)(c). This provision includes no language requiring disclosing parties to contractually impose this obligation on receiving parties; receiving parties' obligation arises directly from the statute itself.

Circumstances Permitting Sale, Lease, and/or Disclosure of Biometric Identifiers

Illinois permits disclosure under certain circumstances, as described below. Texas and Washington permit sale, lease, and/or disclosure under the circumstances described below.

Circumstances	Illinois	Texas	Washington
Consent	Yes	Yes	Yes
Disclosure is required under another law	Yes	Yes	Yes
Disclosure is required pursuant to a warrant, court order, and/or subpoena	Warrant and subpoena	Warrant	Court order
Disclosure is necessary to complete a financial transaction authorized by the individual	Yes	Yes	Yes, if "the third party to whom the biometric identifier is disclosed maintains confidentiality ... and does not further disclose the biometric identifier except as otherwise permitted" by the statute.
Disclosure is consistent with the statute's notice, consent, security, and retention requirements	No	No	Yes
Disclosure is necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual	No	No	Yes
Disclosure is 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 notice and consent requirements	No	No	Yes
Disclosure is made to prepare for litigation or to respond to or participate in the judicial process	No	No	Yes

Source: Lara Tumeh — Bloomberg BNA

Circumstances Chart

Washington has created several additional exceptions to the general bar against disclosure. Disclosure is permitted if it is:

- consistent with the statute's notice, consent, security, and retention requirements;
- ''necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual'';
- ''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 notice and consent'' requirements; or
- ''made to prepare for litigation or to respond to or participate in judicial process.''

§ 2(3). In short, Washington permits disclosure under a significantly broader set of circumstances than do Illinois and Texas.

Finally, the circumstances that permit disclosure in Texas and Washington also permit the sale of biometric identifiers. In contrast, Illinois entirely prohibits the sale of biometric identifiers; it creates no exceptions.

Retention Policies All three state statutes limit businesses' retention of biometric identifiers. They do so in different ways that strike distinct balances between certainty and flexibility.

Washington creates the least certainty and most flexibility by creating a broad retention standard. Specifically, it provides that a business may retain a biometric identifier ''no longer than is reasonably necessary'' to comply with law or a court order; protect against fraud, criminal activity, claims, security threats, or liability; and provide the services for which the biometric identifier was enrolled. § 2(43) (b).

In contrast, Illinois both qualitatively and quantitatively caps retention. Specifically, it requires businesses to destroy biometric identifiers ''when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with the private entity, whichever occurs first.'' 740 ILCS 14/15(a).

Texas combines a broad standard with a quantifiable cap. Specifically, it requires destruction ''within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires,'' absent certain exceptions. Tex. Bus. & Com. Code Ann. § 503.001(c)(3).

Finally, Illinois is unique among the three states in that it requires businesses to publicly post their retention policies in writing.

Enforcement Washington, like Texas, has authorized only the attorney general to enforce the statute. Of the three states, only Illinois has created a private right of action. As a result, BIPA may well continue to be the focus of biometric privacy litigation in the U.S.

Damages Washington defines a violation of its biometric privacy act as an unfair or deceptive act or method of competition, which, under Wash. Rev. Code § 19.86.140, may result in a ''civil penalty of not more than five hundred thousand dollars.'' Texas authorizes damages of $25,000 per violation. Illinois authorizes damages of $1,000, or actual damages, whichever is greater, for negligent violations. It authorizes damages of $5,000, or actual damages, whichever is greater, for intentional or reckless violations. It also provides for attorney's fees.

Consumer Versus Commercial Interests Overall, the three statutes strike different balances between consumer rights and commercial interests. Illinois's is the most consumer-protective in that it includes no commercial purpose limitation, it categorically prohibits the sale of biometric identifiers under all circumstances, it requires written notice and consent, it requires publicly available retention policies, and it creates a private right of action. Washington is arguably the most business-friendly of the three statutes in that it carves out security purposes from its scope, it creates the broadest set of exceptions to the general bar against disclosure to third parties, and it does not create a private right of action.

BY LARA TUMEH

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com