Drinker Biddle

Client Alert

February 14, 2017

Four More States Propose Biometrics Legislation

In recent years, the plaintiffs' class action bar has focused its efforts on pursuing claims under legislative schemes that provide for statutory damages. The litigation explosion under the Telephone Consumer Protection Act ("TCPA") is a textbook example of how enterprising lawyers exploit laws that provide for such uncapped damages in an attempt to extract large settlements for technical violations that, in many cases, have caused no cognizable harm. As plaintiffs begin to explore new claims under these legislative schemes, we seek to help our clients minimize their risk through heightened awareness of the technical requirements of new and existing laws, vigilant compliance programs, and aggressive defense against litigation. Biometrics is one such area.

Last year, we warned of a new wave of potentially high-exposure litigation under Illinois' Biometric Information Privacy Act, 740 ULCS 14/1, *et seq.* ("BIPA"). That wave has included putative class actions against corporate defendants ranging from some of the largest social media and technology companies to a video game manufacturer and even a daycare center. Notably, since January 1, 2017, the Connecticut, New Hampshire, Washington, and Alaska legislatures have also proposed bills that would regulate the collection, retention, and use of biometric data.[1] If passed, these bills could have significant implications for businesses that capture, obtain, store, or use biometric information.

Many of these new legislative proposals borrow from Illinois' BIPA. As one of the first state statutes of its kind, BIPA imposes strict notice and consent requirements on organizations before they may "collect, capture, purchase, receive through trade, or otherwise obtain" biometric identifiers or biometric information (collectively "biometric data"). Specifically, an individual must be given written notice of, and provide written consent to, the initial collection and storage of his or her biometric data as well as the purpose and length of time that data will be stored and used. Any business that collects or obtains such biometric data must (1) develop a written data retention policy available to the public that meets statutory requirements, (2) restrict the transfer or disclosure of biometric data to very limited circumstances, and (3) protect and store that data to, at least, the same degree it protects other confidential or sensitive information. In addition, BIPA creates a private right of action for an "aggrieved person" and provides for statutory damages of $1,000 dollars for each negligent violation and $5,000 for each intentional or reckless violation. As set forth below, the more recently-proposed bills in Connecticut, New Hampshire, Washington, and Alaska contain similar provisions which would likewise create exposure for businesses that collect and use biometric data.

Connecticut

Earlier this year, Connecticut General Assembly Representative Tami Zawistowski introduced a bill that would "prohibit retailers from using facial recognition software for marketing purposes." H.B. 5522, 2017 Gen. Assemb., Reg. Sess. (Conn. 2017). That new proposed house bill comes on the heels of a 2016 bill she co-sponsored that passed the Connecticut house chamber but failed to pass the Connecticut State Senate to become law. The 2016 bill would have required certain retailers to display a sign if they use facial recognition technology to capture any biometric identifier of persons entering their retail locations. H.B. 5326, 2016 Gen. Assemb., Reg. Sess. (Conn. 2016). It broadly defined biometric identifier as "a record of facial geometry, including, but not limited to, an image of an individual's face captured and stored utilizing facial recognition software." And, its signage requirement, if passed, would have applied to "each retail business establishment having a fixed permanent location where goods are offered for sale on a continuing basis." Both the proposed 2016 and 2017 bills follow passage of Connecticut's 2015 Public Act No. 15-142, An Act Improving Data Security and Agency Effectiveness, which bolstered protections under Connecticut's data breach law and expanded the definition of protected personal information to include biometric data such as fingerprints, retina scans, and voice prints.

The public hearing testimony surrounding the 2016 bill demonstrates the competing interests for and against biometrics legislation, which may explain why that bill failed to pass the Connecticut State Senate. Most notably, the technology sector worried the bill's strict notice and consent requirements were too broad and would hinder innovation because "most promising biometric technologies cannot incorporate a notice and consent interface." *See* Memorandum from Matt Mincieli, Northeast Region Executive Director of Technet, on HB 5325, An Act Prohibiting the Capture and Use of Facial Recognition Technology for Commercial Purposes to the General Law Committee (February 23, 2016). It remains to be seen whether the

1 Massachusetts also has a bill before its Senate that would include "biometric indicator(s)" in its regulatory framework governing "personal information." *See* S.B. 750, 190th Gen. Court, Reg. Sess. (Mass. 2017). Specifically, S.B. 750 amends Section 1 of Chapter 93H of Massachusetts' General Laws to include "biometric indicator" within the definition of "personal information." Section 2 of Chapter 93H mandates the department of consumer affairs and business regulations "adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth." "Biometric indicator" is defined as "any unique biological attribute or measurement that can be used to authenticate the identity of an individual, including but not limited to fingerprints, genetic information, iris or retina patterns, voice recognition, facial characteristics or hand geometry."

more recent 2017 bill will be sufficiently tailored to garner enough support to be enacted.

Other States

Much like the Connecticut legislature, lawmakers in New Hampshire, Washington, and Alaska proposed bills related to biometric data earlier this year. *See* H.B. 523, 2017 N.H. H.R., Reg. Sess. (N.H. 2017); H.B. 1493, 2017 Wash. H.R., Reg. Session (Wash. 2017); H.B. 72, 30th Legislature, Reg. Session (Alaska 2017). If passed, all three would regulate the collection, retention, and use of biometric data by individuals or entities. Generally, all three bills would regulate in the following ways. First, they would require notice and consent before an individual's biometric data or information may be collected. Second, all three would prohibit the sale or lease of biometric data and would permit disclosure of biometric data in only a few, enumerated circumstances. Third, the three bills have storage requirements and retention limits to protect the individuals who have their biometric data collected.

a. New Hampshire

On January 5, the New Hampshire house introduced bill number 523, which is very similar to the BIPA. H.B. 523, 2017 N.H. H.R., Reg. Sess. (N.H. 2017). It defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of facial or hand geometry" and excludes from that definition "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color." It also defines "biometric information" to include any information "based on an individual's biometric identifier used to identify an individual," except for any item excluded under the definition of biometric identifier in the bill.

The proposed law would impose a number of restrictions and requirements on individuals and entities that collect, retain, or use biometric identifiers or information. For example, the proposed bill would:

- Require any person who obtains biometric identifiers or information to develop a publicly available written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers or biometric information when the purpose for collection of such data has been satisfied, or within three years of its collection, whichever occurs first;
- Require anyone possessing biometric identifiers or information to protect that data from disclosure in a manner that is at least as protective as the manner in which it safeguards other confidential and sensitive information;
- Prohibit any person from obtaining an individual's biometric identifier or information, unless that person first (a) informs the subject in writing that a biometric identifier or biometric information is being collected or stored; (b) informs the subject in writing of the specific purpose and length of term for which the biometric identifier or biometric information is being collected, stored, and used; and (c) receives a written release from the subject;
- Prohibit "disclosure or re-disclosure" of an individual's biometric identifier or information unless: (a) the subject consents, (b) the disclosure or re-disclosure completes a financial transaction requested and authorized by the subject, (c) the disclosure is otherwise required by state or federal law, or (d) the disclosure is required by a valid warrant or subpoena;
- Prohibit any person from selling, leasing, trading, or otherwise profiting or benefitting from the biometric identifiers or biometric information of any person or customer; and
- Prohibit any person from refusing to conduct business with an individual or customer who refuses to consent to collection, retention, or use of his/her biometric identifiers or information, or who refuses to provide a written release with respect to such data.

As for remedies, the New Hampshire bill, much like BIPA, would create a private right of action for any person "aggrieved" by a violation and would provide for potentially significant statutory damages and fee awards. For each negligent violation, the bill provides for $1,000 in liquidated damages or actual damages, whichever is greater. For each intentional or reckless violation, the bill provides for $5,000 in liquidated damages or actual damages, whichever is greater. In addition, if the proposed bill is passed, an aggrieved person could seek reasonable attorney's fees and costs, and other relief, including injunctive relief, in litigation. The potential exposure for companies that commit innocent transgressions is catastrophic.

b. Washington

On January 20, lawmakers in the state of Washington proposed house bill number 1493. H.B. 1493, 2017 Wash. H.R., Reg. Session (Wash. 2017). That bill defines "biometric identifier" as "data generated by automatic measurements of an individual's biological characteristics" which "uniquely authenticate an individual's identity when the individual accesses a system or account." It includes a "fingerprint, voiceprint, eye retinas or irises, or other unique biological characteristic." The bill would require "clear and conspicuous notice" and the "individual's consent" (1) before a biometric identifier can be enrolled in "a database to create identification of an individual" and (2) before an already enrolled biometric identifier can have its use changed. According to the bill, clear and conspicuous notice is a "context-dependent" standard that is achieved "through a procedure reasonably designed to be prominent, timely, relevant, and easily accessible." It allows retention to last "no longer than reasonably necessary" to "effectuate the purpose for which the individual has provided consent," to "comply with court order, statute, or administrative rule," or to protect against or prevent "fraud, criminal activity, claims, security threats, or liability." Furthermore, under the bill, a person cannot "sell, lease, or otherwise

disclose" a biometric identifier unless an enumerated exception applies. A person who enrolled a biometric identifier for a commercial purpose must also "take reasonable care to guard against unauthorized access to the biometric identifiers that are in the possession or under the control of that person."

c. Alaska

On January 20, the Alaskan legislature proposed house bill 72 on the issue of biometrics. H.B. 72, 30th Legislature, Reg. Session (Alaska 2017). The 2017 Alaskan bill defines biometric data as "fingerprints, handprints, voices, iris images, retinal images, vein scans, hand geometry, finger geometry, or other physical characteristics of an individual." It also defines biometric information as "biometric data used in a biometric system." That bill requires that notice be provided "in a clear manner" to disclose the following: (1) the fact that biometric data is being collected for use in a biometric system; (2) the specific purpose for which the biometric data will be used; and (3) the length of time the biometric data will be retained. *Id.* Additionally, consent to the above must be "full consent" documented in "written, electronic, or other form [for documentation]." Under the bill, a person "may not sell biometric information, except that a contractor may sell the contractor's business to another person and transfer the biometric information to the buyer." Both collectors and contractors must store biometric information "in a secure manner, which may include encryption or another appropriate method, to ensure that the identity of the individual who provided the biometric information is protected." The bill requires disposal of biometric information within 120 days after "a collector no longer needs an individual's biometric information for the original purpose for which the biometric information was going to be used" "unless prohibited by other law, a regulation, or a court order." Finally, with respect to remedies, the Alaskan bill sets forth $1,000 in statutory damages for intentional violations. *Id.* Such statutory damages increase to $5,000 per intentional violation if the violation results in "profit or monetary gain."

* * *

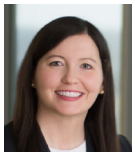
Although these four proposed state laws are still in the early stages of the legislative process, they exemplify the trend toward growing regulation of biometric data and technology. As the uses of biometric data continue to expand, companies should be vigilant about monitoring such proposed legislation. If these kinds of statutes proliferate state to state, the costs for noncompliance are potentially too significant to ignore. To that end, companies seeking to mitigate risk should consider taking a number of steps:

- Drafting and revising corporate policies and procedures to govern collection, storage, safeguarding, handling and use of biometric data.
- Developing a program to remediate any identified gaps and upgrading data security controls as needed to protect biometric data as confidential and sensitive information, whether captured from consumers or employees.
- Updating the compliance program to reflect statutory requirements as laws develop.
    - Develop a written policy for retention and regular destruction of biometric data;
    - Put in place a comprehensive process to inform consumers about the collection, storage and use of biometric data and for obtaining the requisite consent;
    - Ensure any biometric data is adequately protected from inadvertent disclosure; and
    - Refrain from selling biometric data or sharing it with third parties, unless you are sure doing so is permitted by applicable law.

If you have any questions about best practices or the legislative proposals addressed in this alert, please do not hesitate to contact the authors or your usual Drinker Biddle contact.

Litigation Group

Primary Contacts



Kathryn E. Deal
Partner
Philadelphia
(215) 988-3386
Kathryn.Deal@dbr.com

Justin O. Kay
Partner
Chicago
(312) 569-1381
Justin.Kay@dbr.com

Meredith C. Slawe
Partner
Philadelphia
(215) 988-3347
Meredith.Slawe@dbr.com

Drinker Biddle®

www.drinkerbiddle.com

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | TEXAS | WASHINGTON DC | LONDON

© 2017 Drinker Biddle & Reath LLP. All rights reserved. A Delaware limited liability partnership. Promotional Materials 2017. One Logan Square, Ste. 2000, Philadelphia, PA 19103-6996 (215) 988-2700 *office* (215) 988-2757 *fax*
Jonathan I. Epstein and Andrew B. Joseph., Partners in Charge of the Princeton and Florham Park, N.J., offices, respectively.