

Getting Personal: Biometric Privacy Laws Are on the Rise

Biometric data laws are growing as part of the privacy landscape in the United States. As physical biometric data increasingly becomes a preferred means of identification by many businesses, and particularly by employers, consumer protection concerns abound and state legislators have been struggling to find an appropriate balance.

While there is no uniform federal biometric data privacy law, several states in the United States, including Illinois, Oregon, Texas, California, Washington and New York, either have existing laws or are in the process of drafting new laws. Although it remains to be seen how such legislation will change the reliance upon and use of biometric data, it is clear that there is a need for businesses to implement formal data security and privacy frameworks, such as written policies, with respect to the collection and use of biometric data, whether or not required by law.

Private Rights of Actions

The Illinois Biometric Information Privacy Act (BIPA) (the first comprehensive biometric data law in the United States) is the only state law actually in effect that expressly affords individuals a private right of action. As a result, BIPA has become a favorite tool of class action lawyers and an expensive problem for businesses.

Other city-level regulations, such as was enacted in Portland, Oregon in January 2021, also provide private rights of action. Portland's city-wide ordinance prohibits the use of facial recognition technology by private entities in places of public accommodation. One challenge now facing affected businesses in Portland is that there is uncertainty around what constitutes "facial recognition technology," as well as whether informed consent creates an exception to the prohibition. Similarly, in June 2021, the city of Baltimore enacted a Private-Sector Face Surveillance System Ban, banning the use of facial recognition technology by individuals and private businesses within the city.

BPA

Also in January 2021, the New York State Legislature proposed the Biometric Privacy Act (BPA), seeking to enhance the privacy rights of individuals via the implementation of controls around the collection and processing by private entities of biometric information. New York City also passed a law requiring commercial establishments to post clear disclosures at all

entrances where consumers might enter, notifying them of the collection, use and/or sharing of their biometric information.

Although several states have proposed biometric data legislation that has not advanced, it is likely that lawmakers will continue to be active and applicable laws will continue to evolve.

What Businesses Can Do Now

- The confluence of privacy, security and societal concerns have resulted in increased scrutiny over the use of biometric data.
- In the absence of a consistent federal standard, and in anticipation of increased state regulation, businesses should assess their practices and formalize their policies with respect to the collection and use of biometric data.
- As a general best practice, notice and consent should be given and received prior to collecting and using biometric data.



Gary Kibel

Partner
gkibel@dglaw.com

For companies operating at the intersection of digital media, advertising, technology and ... [more](#)



Oriyan Gitig

Counsel
ogitig@dglaw.com

With Oriyan's counsel, creative agencies and technology companies understand and uphold privacy ... [more](#)