D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

JANUARY 2021

DIGITAL MEDIA, TECHNOLOGY & PRIVACY
>> ALERT

DON'T SMILE AT THE CAMERA — NEW BIOMETRIC DATA LAWS

Biometric data is seen as a preferred means of identification by many businesses.

Unlocking a smartphone using facial recognition and other biometric identifiers, for example, gives users the feeling as if they are more protected (*e.g.*, less risk of identity theft). However, similar to the boom in privacy developments and legislation related to the collection and use of more traditional personal information, the growth of biometric data use by businesses, law enforcement, employers and other organizations has given rise to renewed privacy concerns and legal developments.

While there is no uniform federal biometric data privacy law, several states either have existing laws or are in the process of drafting or ratifying new laws. Although it remains to be seen how such legislation will change the industry's use of and reliance upon biometric data, that it is increasingly the subject of analysis and discussion indicates a demand and a need for reasonable security and privacy practices around the collection and processing of biometric data, whether required by law or not.

EXISTING STATE LAWS — ILLINOIS

While several states, including Texas, Washington, California, New York and Arkansas have existing laws that directly govern or otherwise address biometric data in some fashion, only one, Illinois, has a comprehensive law that offers a private right of action to *aggrieved* individuals. The Illinois Biometric Information Privacy Act (BIPA) imposes rigorous requirements on businesses that collect or otherwise process biometric data, including, requiring consent from the consumer before the collection, and disclosure of their policies regarding use and retention, of such data.

Unique to BIPA is the individual's private right of action, whether actually injured or not by the BIPA violation. In *Rosenbach v. Six Flags Entertainment Corp.*, the Illinois Supreme Court held that a violation of BIPA alone, regardless of damage or injury, is enough to give rise to such private right of action. If found to be in violation of BIPA, penalties (on a per-violation basis) may range from $1,000 to $5,000. As a result, BIPA has become a favorite tool of class action lawyers and an expensive issue for businesses.

THE BOTTOM LINE

The confluence of privacy, security, societal and other reasons have resulted in increased scrutiny over the use of biometric data through new proposed laws. In the absence of a consistent federal standard, businesses should assess their biometric data collection and use practices and technologies, implement a written policy, plan for the collection and use of such data, and ensure disclosures and consents, as appropriate, are given to and received by individuals whose data is collected.

NEW AND PENDING STATE LAWS — OREGON & NEW YORK

The City of Portland, Oregon, enacted a city-wide ordinance on January 1, 2021 prohibiting (with a few exceptions, *e.g.*, for compliance with law and user verification purposes) the use of facial-recognition technology by private entities in *places of public accommodation* (which are defined as, "any place or service offering to the public accommodations, advantages, facilities or privileges whether in the nature of goods, services, lodgings, amusements, transportation or otherwise.").

>> continues on next page

Notably, in addition to standard privacy concerns, the genesis of this statute seems to have derived from a concern that all residents and visitors of the city be treated fairly and equally with respect to surveillance and the use of biometric data, as well as growing evidence that some uses of facial recognition technologies have resulted in misidentification and biased practices with respect to race and gender.

There is some uncertainty around what constitutes "facial-recognition technology," as well as whether informed consent creates an exception to the prohibition since the ordinance does not address how an individual's consent to the collection and use of such data would impact the prohibitions. Similar to BIPA, the Portland ordinance also provides for a private right of action, with penalties up to $1,000 per day for each day of the violation.

On January 7, the New York State Legislature proposed the Biometric Privacy Act (BPA). Whereas the Portland ordinance prohibits outright the use by private entities of facial recognition technologies, the BPA seeks instead to enhance the privacy rights of individuals and controls around the collection and processing by private entities of biometric information.

Prior to collection, the individual must be informed of the:

- Specific biometric data to be collected,
- Purpose and duration of the collection and use, and
- Individual must give written consent to the foregoing.

Additionally, the BPA imposes restrictions on the use and disclosure of such biometric data by the entity that collected or otherwise received it. The BPA also provides "aggrieved" individuals with a private right of action with penalties ranging from $1,000 to $5,000 (or, if greater, actual damages).

FOR MORE INFORMATION

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

Oriyan Gitig
Counsel
212.468.4880
ogitig@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
212.468.4800
1675 Broadway, New York, NY 10019
www.dglaw.com

© 2021 Davis & Gilbert LLP