You looking at me? — cameras, devices and biometric data

By Gary Kibel, Esq., Davis+Gilbert LLP

MAY 20, 2022

Data collection and privacy issues often are focused on the online world. Websites, mobile apps and electronic devices of all kinds are collecting information on their users and are leveraging that data for various business purposes, such as marketing and advertising. Lawmakers and regulators often focus their privacy enforcement efforts at this online world. However, there is an ever-increasing industry of collecting data in the offline world, and laws are starting to catch up with these practices.

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, like 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.

New comprehensive consumer privacy laws

As of the writing of this article, five states in the United States have enacted comprehensive consumer privacy laws: California, Virginia, Colorado, Utah and Connecticut. All five state laws define "sensitive data" in one form or another, and each one includes biometric data as a form of such sensitive data. That designation triggers differing obligations under each law.

Virginia, Colorado and Connecticut require consent from the data subject before a business can collect and process such biometric data. Some of the laws also require that a business conduct a data privacy impact assessment regarding the processing of such sensitive data. For businesses that have typically operated on an opt-out model, this will require significant changes to business practices when these new laws take effect in 2023.

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.

Like 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.

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. Definitions often drive these laws, since there is no commonly accepted or intuitive definition of biometric data. The definition under BIPA only includes "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." Some other laws have broader definitions.

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.

New and pending state laws — Oregon and New York

The City of Portland, Ore., enacted a city-wide ordinance on Jan. 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.").

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.

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. Like BIPA, the Portland ordinance also provides for a private right of action, with penalties of up to $1,000 per day for each day of the violation.

New York City adopted a biometric data law that merely requires physical signage in a place of public accommodation that collects physiological or biological characteristics used to identify an individual, including retina/iris, fingerprint/voiceprint and scan of hand/facial geometry, such as through a security camera.

Specifically, the law states that "[a]ny commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such....by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language.... that customer's biometric identifier information is being collected."

Conclusion

The confluence of privacy, security, societal and other reasons have resulted in increased scrutiny over the use of biometric data through new and 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 appropriate disclosures and consents are given to and received by individuals whose data is collected in compliance with all such laws.

Gary Kibel is a regular contributing columnist on data privacy for Reuters Legal News and Westlaw Today.

About the author

Gary Kibel is a partner at **Davis+Gilbert LLP**, where he is a member of the Privacy + Data Security and Advertising + Marketing practice groups. He provides clients perspective on cutting-edge issues in digital media, advertising, technology and privacy. He is based in New York and can be reached at gkibel@dglaw.com.

This article was first published on Reuters Legal News and Westlaw Today on May 20, 2022.