

# A National Biometric Privacy Law? Laws Protecting “Biometric” Identifiers Continue to Cut a Blazing Trail

*Amundsen Davis Data Privacy & Security Alert*  
August 19, 2020

This month, federal legislation aimed at protecting biometric data was introduced in the U.S. Senate. If it passes, the National Biometric Information Privacy Act of 2020 would be the first comprehensive federal law on biometric data. Specifically, it would prohibit private businesses from collecting faceprints, fingerprints, retina scans, voiceprints, and other biometric data, without first having the consumers’ or employees’ consent. It would also limit companies’ collecting, buying, selling, leasing or trading biometric data without written consent and hold businesses to very specific disclosure requirements on biometric data collected. The law would also pack a significant punch for failure to comply: private causes of action could range from \$1,000-\$5,000 “per violation,” a statutory remedy that could mushroom given the potential volume of biometric data collected.

## **I thought biometric laws already existed?**

What the federal law proposes is really nothing new—certainly not for residents in California, Illinois, Texas, Washington and other states that already have biometric privacy laws. The state-mandated requisites for collection and use of biometric data are already on the forefront of many companies’ minds as they navigate the California Consumer Privacy Act (CCPA), Illinois’ Biometric Information Privacy Act (BIPA), and other states’ regulations and protections. However, state laws only impact businesses if they conduct business in or engage with residents of a particular state. The National Biometric Information Privacy Act would mean a broader protection, subjecting companies in all trades and industries to strict biometric data compliance.

## **Why is there now a federal push for regulation?**

The concern over and a desire to protect biometric data has only continued to increase and intensify. And, at the same time, the technology that captures “biometric data” and the touch-points where that data may be collected has been expanding. As technology continues to advance, more businesses are utilizing

## **PROFESSIONALS**

Molly A. Arranz  
Partner

## **RELATED SERVICES**

Biometric Privacy  
Cybersecurity & Data Privacy

biometrics to enhance customer experience, better track employees, and enhance security. But like all new technology, there are growing concerns around how biometric data is being used – particularly in regard to facial recognition. For example, Rite Aid recently faced public scrutiny for its use of facial recognition technology to heighten security measures and deter theft amongst its retail stores because questions were raised about whether the technology misidentified individuals of color. Additionally, because biometric information is uniquely sensitive and cannot be changed, the public is increasingly showing more interest and concern over how their information is being used and exactly what information is being collected. Given all of this, it was likely only a matter of time until lawmakers on the federal level teed up legislation.

### **What does this mean for my business moving forward?**

The National Biometric Information Privacy Act has only been introduced, so depending on your data collection “reach” by state, the current, biometric data laws may not subject your company to any official requirements. However, the concern over biometric data is not going away, and as a matter of best business practice, you should consider:

1. Whether your business is currently collecting biometric data—a term that has been broadly interpreted;
2. If your business is collecting biometric data, how and why you are using this data;
3. Whether it makes financial and practical sense to leverage your existing policies to address the use and collection of biometric data; and,
4. If you aren’t currently obtaining consent and making the disclosures about this set of data, the financial (and public relations) fall-out for not doing so.

Generally speaking, compliance with laws protecting biometric data can be very straightforward, especially given the policies and disclosures companies are already making. Getting ahead of the curve on these new laws, now, could save you headaches—and money—down the road.

A National  
Biometric  
Privacy  
Law? Laws  
Protecting  
“Biometric”  
Identifiers  
Continue to  
Cut a  
Blazing Trail