Updates
June 21, 2022

Getting the Right Fit: Biometric Privacy and the Apparel Industry

In recent years, apparel and retail businesses have increasingly sought to provide customers with options to interact with the brand's merchandise and services in virtual environments. This includes everything from virtual try-on to virtual stores in the metaverse. Depending on their specific nature, these services could potentially trigger biometric privacy laws, generating risk for businesses. Indeed, dozens of cases have been filed contending that apparel or retail businesses violated biometric privacy laws in providing virtual try-on or other similar services.

A growing number of state laws regulate the collection, use, and disclosure of biometric data. The two most notable laws are the Illinois Biometric Information Privacy Act (BIPA) and the Texas Capture or Use of Biometric Identifier law (CUBI). BIPA and CUBI regulate "biometric identifiers," including retina or iris scans, fingerprints, voiceprints, and "scans" (BIPA) or "records" (CUBI) of hand or face geometry. BIPA also regulates "biometric information," which is information based on a biometric identifier used to identify a specific individual. The laws impose slightly different requirements on businesses that collect biometric data, including notice and consent requirements, limitations on sharing, limitations on retention, and data security requirements, among others. BIPA allows private parties to sue for violations and has generated over 1,500 class actions in just the last six years.

Careful and thoughtful consideration of key biometric privacy principles can help mitigate risk in this area. Accordingly, when designing these services, brands should consider the following issues:

- **Does the service involve biometric data?** Although the definition of what constitutes "biometric" data varies from jurisdiction to jurisdiction, services that measure or scan customers' hands, faces, eyes, or other features could potentially include biometric data. In some cases, voice recordings and other voice data could also be considered biometric data. Given the varying definitions across jurisdictions, businesses should obtain advice from experienced biometric privacy counsel to determine whether biometric data is involved.
- **Is notice or consent required?** Some jurisdictions may require a business to give advance notice and obtain consent before collecting, processing, or sharing biometric data. These laws may be triggered in some cases even if the data is processed quickly and immediately discarded. The specific language to provide notice and obtain consent must be carefully crafted to comply with applicable law.
- **Are there limits on retention?** Some jurisdictions limit how long a business may retain biometric data. These time limitations are often tied to the expiration of the purpose for which the biometric data was collected. Some laws, like BIPA, also require companies to publish retention and deletion schedules. Accordingly, businesses must carefully craft their retention and deletion policies as applied to biometric data.
- **Are appropriate physical or digital security measures in place?** Finally, relevant laws may require businesses to implement physical and digital security measures to protect the biometric data they collect. Businesses designing data security measures to meet these requirements must take care to consider relevant industry standards, as well as controls the businesses may already be using to protect other sensitive data.

Perkins Coie's team of biometric law attorneys have deep experience advising clients on the use and development of biometric technologies and litigating cases relating to biometric data and biometric privacy. For

further information, do not hesitate to reach out to biometrics@perkinscoie.com or contact one of the authors.

Authors

Nicola Menaldo

Partner
NMenaldo@perkinscoie.com 206.359.8000

Justin Potesta

Counsel
JPotesta@perkinscoie.com 737.256.6137

Explore more in

Privacy & Security Retail & Consumer Products Apparel & Footwear Outdoor

Related insights

Update

FERC Meeting Agenda Summaries for October 2024

Update

New White House Requirements for Government Procurement of AI Technologies: Key Considerations for Contractors