Virtual ‘Try On’ Features: Do They Create Biometric Privacy Concerns for Retailers?

Article By

Marlén Cortez Morris
Zachary V. Zagger

Ogletree, Deakins, Nash, Smoak & Stewart, P.C.
Our Insights

Related Practices & Jurisdictions

- Communications, Media & Internet
- Consumer Protection
- All Federal

Thursday, August 11, 2022

Retailers’ virtual “try-on” features have come under attack lately by lawsuits claiming violations of consumers’ biometric privacy rights. The increasing risk of litigation highlights a new area of compliance concern for retailers as online shopping has become the new normal for many consumers.

Typical lawsuits in this space concern the popular online virtual “try on” features offered by a variety of retailers, including eyewear, fashion, and cosmetics brands,
which allow consumers—from the comfort of their homes—to view what products will look like on their faces or bodies before making a purchase. Consumers either upload an existing photograph or use their phone or computer camera to see, for example, what a particular pair of glasses might look like on their faces, or what a certain color of lipstick might look like once applied. Retailers are increasingly using these tools, which became particularly popular during the pandemic, as a substitute for the traditional in-store experience, to enable shoppers to “try on” and buy products virtually.

Recently, plaintiffs’ attorneys have filed lawsuits alleging that these virtual tools implicate consumers’ biometric privacy rights because they use and collect consumers’ biometric information, such as facial geometry, and that retailers are not properly disclosing to consumers that such information is being collected and potentially stored. These lawsuits have primarily targeted optical and makeup retailers and are testing the scope of Illinois’ Biometric Information Privacy Act (BIPA) and other privacy laws to ascertain whether these laws’ safeguards on biometric privacy apply in this context.

Illinois became the first state to pass comprehensive—and the most stringent—biometric privacy legislation with the passage of BIPA in 2008. The law regulates private entities’ collection, use, storage, transmission, and destruction of “biometric identifiers,” which the law defines as “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.”

The law prohibits private entities from collecting biometric information without first informing the person from which data is being collected “in writing” that the data is being collected, disclosing the “specific purpose and length of the term for which” the data is being collected and stored, and obtaining written consent. BIPA further requires private entities in possession of biometric data to “develop a written policy, made available to the public, establishing a retention schedule and guidelines” for the timely destruction of the data. BIPA also restricts the sale and disclosure of biometric information. Significantly, BIPA provides a private right of action for any “person aggrieved” by a violation of the law and allows the recovery of statutory damages in the amount of $1,000 per negligent violation, $5,000 per intentional violation, actual damages, injunctive relief, and attorneys’ fees and costs.

Illinois courts have interpreted BIPA broadly to allow class actions to move forward even when there have been only technical violations of the law, such as where companies failed to meet the relevant disclosure and written consent requirements. Similarly, although BIPA excludes photographs (and information derived from photographs) from its scope, courts have also declined to exclude biometric information derived from photographs from the law’s reach given its coverage of facial geometric scans.

Beyond Illinois, a number of states and cities have biometric privacy laws that could apply to the use of virtual try-on technology. A growing number of states, including California, Maryland, and New York, are also considering comprehensive biometric privacy laws modeled on BIPA that could create additional requirements for notice and storage of biometric data and provide consumers private rights of action.
In the face of these lawsuits, some retailers have argued that biometric data is not being stored or that the claims are subject to arbitration agreements included in the terms of service applicable to use of their websites and the virtual try-on tools. In one suit against several eyeglass and makeup retailers, one of the companies argued that consumers agree to arbitration simply by visiting its website because the website displays “conspicuous” hyperlinks to its terms of use on each page. The suit was dismissed before the court could decide this question. Thus, it remains to be seen whether such terms of service would apply and whether the notice of the terms provided to consumers would comply with BIPA’s informed consent requirements.

In addition to their popularity, virtual try-on tools are also rapidly advancing and in some contexts can be combined with artificial intelligence (AI) technology to generate recommendations based on consumers’ preferences and their individual biometric profiles, such as face shapes and body types. Because this practice implicates the storage and analysis of biometric data collected from consumers, it could trigger application of biometric privacy or other privacy laws.

Key Takeaways

Retailers using virtual try-on technology may want to review their practices and policies to determine whether they are storing or using any biometric information (or information derived from it) to generate recommendations or tie preferences to consumers’ shopping profiles, and if so, take appropriate steps to ensure compliance with applicable biometric privacy and other privacy laws. They may also want to consider updating terms and conditions for use of their websites to provide notice of biometric data collection and disclosure. To facilitate compliance and dispute resolution, retailers doing business online may also want to evaluate alternative dispute resolution options and consider whether to include pop-up notifications with disclosures that consumers must accept before they are allowed to use the virtual try-on tools.

Ogletree Deakins will continue to monitor this wave of biometric privacy class action litigation and post updates to the Retail and Cybersecurity and Privacy blogs. Important information for employers is also available via the firm’s webinar and podcast programs.
