BCLP. Client Intelligent

Insights

FTC POLICY STATEMENT ON BIOMETRIC INFORMATION AND TECHNOLOGY

May 26, 2023

The Federal Trade Commission ("FTC") has issued a policy statement addressing biometric technologies in a signal of enforcement actions to come. It states: "In light of the evolving technologies and risks to consumers, the Commission sets out . . . examples of practices it will scrutinize in determining whether companies collecting and using biometric information or marketing or using biometric information technologies are complying with Section 5 of the FTC Act [unfair or deceptive acts or practices]."

Companies who have not been "clocking" the mass wave of biometric privacy-related class action litigation or the biometric-specific statutes in Illinois, Texas, and Washington, need to take heed. Even for those businesses who have a biometric privacy policy in place, the FTC made express: "Compliance with those [state or city biometric] laws . . . will not necessarily preclude Commission law enforcement action under the FTC Act or other statutes."

WHAT TYPE OF INFORMATION DOES THE FTC POLICY STATEMENT COVER?

The Policy Statement defines "biometric information" as:

> data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body. Biometric information includes, but is not limited to, depictions, images, descriptions, or recordings of an individual's facial features, iris or retina, finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern). Biometric information also includes data derived from such depictions, images, descriptions, or recordings, to the extent that it would be reasonably possible to identify the person from whose information the data had been derived. By way of example, both a photograph of a person's face and a facial recognition template, embedding, faceprint, or other data that encode measurements or characteristics of the face depicted in the photograph constitute biometric information.

WHAT SHOULD BUSINESSES BE DOING IN THE WAKE OF THE FTC'S POLICY STATEMENT?

- Implement privacy and data security measures to ensure that any biometric information collected or maintained is protected from unauthorized access;
- Conduct a "holistic assessment" of potential risks to consumers associated with the collection and/or use" of consumer's biometric information before deploying biometric information technology;
- Promptly address known or foreseeable risks (*ie.* if biometric technology is prone to certain types of errors or biases, businesses should take steps to reduce those errors or biases);
- Disclose the collection and use of biometric information to consumers in a clear, conspicuous, and complete manner;
- Have a mechanism for accepting and addressing consumer complaints and disputes related to the use of biometric information technology;
- Evaluate the practices and capabilities of service providers and other third parties that will be given access to consumers' biometric information or that will be charged with operating biometric technology or processing biometric data. Contractual requirements may not be enough; strategic, periodic audits should be considered. As the FTC states: "Businesses should seek relevant assurances and contractual agreements that require third parties to take appropriate steps to minimize risks to consumers. They should also go beyond contractual measures to oversee third parties and ensure they are meeting those organizational and technical measures (including taking steps to ensure access to necessary information) to supervise, monitor, or audit third parties' compliance with any requirements";
- Provide appropriate training for employees and contractors whose job duties involve interacting with biometric information or biometric technology; and
- Conduct "ongoing monitoring" of biometric technologies used—"to ensure that the technologies are functioning as anticipated, that users of the technology are operating it as intended, and that use of the technology is not likely to harm consumers."

HOW DO THESE REQUIREMENTS DIFFER FROM THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT?

The FTC will be looking for businesses to have collected a "'holistic assessment' of potential risks to consumers associated with the collection and/or use" of consumer's biometric information before deploying biometric information technology and to conduct "ongoing monitoring" of

technologies used. These are not requirements codified in the Illinois BIPA or any other state or local biometric law.

While existing biometric and broader consumer privacy statutes require reasonable data security measures, the FTC's Policy Statement suggests businesses should also have training programs regarding the use of biometric technology.

HAS THE FTC BROUGHT ENFORCEMENT ACTIONS OVER BIOMETRIC TECHNOLOGIES?

Yes. In 2021, the FTC settled its action against a photo app developer alleging that the developer deceived consumers about use of facial recognition technology and the developer improperly retained photos and videos of users who deactivated their accounts. The settlement reached included 20 years of compliance monitoring. The FTC also charged a social media company with eight privacy-related violations, which included allegations of misleading consumers about a photo-tagging tool that allegedly used facial recognition. That matter settled for $5 billion in 2019.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Business & Commercial Disputes
- International Trade

MEET THE TEAM

Lauren J. Caisman

Chicago

lauren.caisman@bclplaw.com
+1 312 602 5079

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2024 Bryan Cave Leighton Paisner LLP.