JENNER & BLOCK

# Client Alert: FTC Signals Greater Scrutiny of Biometric Information and Technologies in New Policy Statement

**Publications**

May 30, 2023
By: Madeleine Findley, David C. Layden

On May 18, 2023, the Federal Trade Commission (FTC) adopted a Policy Statement on biometric information that details its "significant concerns" arising from the increasing use of biometric information and technologies that use (and "purport to use") biometric information. The statement also affirms the FTC's commitment "to combatting unfair and deceptive acts" related to the collection and use of biometric information and marketing and use of biometric technologies. The Policy Statement outlines the FTC's view that Section 5 of the FTC Act provides authority over consumer protection risks related to biometric information and provides a non-exhaustive list of factors the FTC will consider when examining business practices. Given the broad sweep of what the FTC views as "biometric information" and the factors it identifies as pertinent to whether a business has engaged in unfair or deceptive acts—both of which go beyond obligations under existing state and local laws—businesses should be aware of the Policy Statement and evaluate how the FTC's pronouncements may impact their development, marketing, sale, and use of such technology.

**FTC's Concerns.** The FTC notes that biometric technologies have become more advanced and more affordable, incorporating machine learning and enhanced data processing capabilities, and "increasingly pervasive." The Policy Statement provides examples of consumer protection concerns, including that biometric information can be used to create deepfakes to commit fraud or harassment, that large databases of biometric information may be attractive targets for malicious actors, that the use of biometric technologies may reveal sensitive personal information about consumers' locations, including that they accessed certain types of healthcare or attended religious services, and that some biometric technologies perform differently across different demographic groups and when the subject is a person with a disability—leading to discriminatory outcomes.

**FTC's View of What Constitutes "Biometric Information."** In the Policy Statement, the FTC articulates a very broad definition of "biometric information":

> As used in this document, the term "biometric information" refers to 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.

The FTC's view of what constitutes "biometric information" goes beyond the scope of existing state and local privacy laws (e.g., by including photographs and voice recordings as biometric information). In addition, the FTC expressly declines to limit its scrutiny to technologies that are used to identify individuals; instead, it makes clear that the Policy Statement applies to "all technologies that use or purport to use biometric information for any purpose."

The FTC provides a non-exhaustive list of practices involving the collection and use of biometric information that it "will scrutinize in determining whether companies collecting and using" or "marketing" biometric information technologies are complying with Section 5 of the FTC Act.

**Deception.** The Policy Statement highlights two practices that may constitute deceptive practices in violation of Section 5:

- ***False or unsubstantiated marketing claims relating to the "validity, reliability, accuracy, performance, fairness, or efficacy" of biometric information technologies.*** The FTC states that such claims may mislead consumers and competitors by making false claims about a product's capabilities and then cause harm when the product does not work as promised or denies benefits or opportunities to consumers. For example, the FTC cautioned businesses not to make claims about a technology's efficacy or accuracy if the claims are based on tests or audits that do not replicate real-world conditions or if the tests results are only true for a certain subset of the population.

- ***Deceptive statements about the collection and use of biometric information.*** The FTC says it will continue scrutinizing businesses to ensure that they are not making false statements or telling "half-truths" to consumers about whether or when biometric information is collected and how businesses use such information.

**Unfairness.** The Policy Statement describes ways that the use of biometric information or biometric technologies may be an unfair practice under Section 5, especially when they cause harms that consumers cannot reasonably avoid and are not outweighed by countervailing benefits to consumers or competition. The FTC identifies in particular the surreptitious collection and use of biometric information, the failure to protect consumer personal information with reasonable data

security practices, implementing privacy-invasive default settings, and disseminating or selling inaccurate technology or technology with the potential to cause harmful or illegal conduct without taking reasonable measures to prevent such conduct. When examining a business's use of biometric information or biometric technology, the FTC will consider non-exhaustive factors such as:

- ***Failing to assess foreseeable harms to consumers associated with collecting and using biometric information.*** The FTC expects businesses that collect biometric information or use biometric technology to conduct a "holistic assessment of the potential risks to consumers" before collecting such information or deploying such technology. Such assessments should consider the context of the collection or use, what role a human operator will have, and whether using a biometric information technology system would lead or contribute to a disproportionate harm to certain groups within the population.

- ***Failing to promptly address known or foreseeable risks.*** The FTC will look for businesses to identify and implement readily available tools to identify, reduce, or eliminate risks. This includes adopting organizational and technical measures and being informed of and taking proactive measures to identify and reduce risks of common errors and biases produced by the biometric information technologies they use.

- ***Engaging in surreptitious and unexpected collection or use of biometric information.*** The FTC says that collecting or using biometric information or biometric information technology in ways that may cause risks of harm to consumers, including stalking or extreme emotional distress, or that makes collection or use unavoidable, including failing to clearly and conspicuously disclose the information collection and using or failing to provide a complaint mechanism, may be unfair practices.

- ***Failing to evaluate the practices and capabilities of third parties.*** The FTC additionally expects businesses to seek assurances and contractual agreements from third parties, including affiliates, vendors, and end users, to minimize risks to consumers of access to biometric information or biometric information technology. And businesses "should also go beyond contractual measures to oversee third parties," including through organizational and technical measures for supervision and monitoring.

- ***Failing to provide appropriate training for employees and contractors regarding the collection and use of biometric information.*** Businesses will be expected to provide training to workforce members interacting with biometric information or biometric information technology.

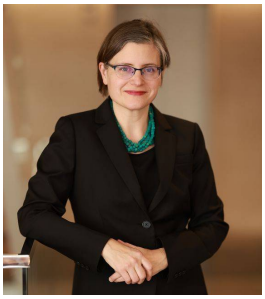
- ***Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or uses in connection with biometric information.*** The FTC states that businesses should monitor technologies developed, sold, or used in connection with biometric information

on an ongoing basis to ensure that users of the technology are operating it as intended and use of the technology is "not likely to harm consumers."

It may prove challenging for businesses to determine whether the Policy Statement applies to their activities—given the broad scope of the FTC's view of "biometric information" and its stated intent to scrutinize technologies beyond those used to identify people. It may be equally challenging, as a practical matter, to apply the FTC's views of the practices that are deceptive and unfair. For example, the FTC's statements about the necessity of technology providers conducting ongoing monitoring of not only their vendors and affiliates, but also their customers and end users of the technology do not account for the significant practical challenges and barriers associated with implementing such monitoring.

That said, recognizing what the Policy Statement signals about the FTC's intent to more actively regulate biometric technologies and with the expectation that the views expressed here will inform the agency's approach to investigations and enforcement actions, it is important for any business that provides or uses technologies that may fall within the FTC's field of view to consider whether to take any action in response to the Policy Statement.

## Related Attorneys

**Madeleine Findley**
Partner
mfindley@jenner.com
+1 202 639 6095

**David C. Layden**
Partner
dlayden@jenner.com
+1 312 923 2796

## Related Capabilities

Data Privacy and Cybersecurity



**Stay Informed** →