

FTC Adopts Policy Statement on Biometric Data

May 23, 2023

During the Federal Trade Commission's (FTC) Open Meeting on May 18, the Commissioners unanimously voted to adopt the [Policy Statement on Biometric Information and Section 5 of the FTC Act](#). The Policy Statement broadly defines biometric data, catalogues the risks the Commission believes are posed by technology that utilizes biometric information, and imposes substantive requirements on companies employing these technologies.

The Policy Statement refers to biometric information as data in the form of depictions, images, descriptions, or recordings of "physical, biological or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body." The scope of such information includes what typically comes to mind when consumers think of biometric data (e.g., facial recognition, iris or retina, fingerprints or handprints, genetics, voice), but also characteristics of movement or gesture like gait or typing pattern. Such information also includes data derived from the depictions, images, recordings, etc., to the extent it would be "reasonably possible" to identify the consumer from whom the original information was derived. The Policy Statement provides an example of biometric information, referring to a facial recognition template that encodes measurements or characteristics of a consumer's face that was derived from her photograph.

It also highlights risks posed to consumers by biometric technologies, including: revealing sensitive information about individuals (e.g., attendance at political events), fraud (e.g., using consumer's images in deepfakes), and, most importantly, bias that leads to harmful or illegal discrimination. Large databases of biometric information may also be an attractive target for other illicit uses by malicious actors. The FTC broke down the practices it will examine for potential violations of Section 5 of the FTC Act (*see below*), but a major development is that the FTC is essentially requiring companies using biometric information to undertake risk assessments before they collect or use biometric information or deploy biometric information technology.

The Statement specifies the practices the Commission will scrutinize in determining whether companies are compliant with Section 5:

- ***False or unsubstantiated claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information.***
- ***Deceptive statements about the collection and use of biometric information.***
- ***Failing to assess foreseeable harms to consumers before collecting biometric information.***
- ***Failing to promptly address known or foreseeable risks.***
- ***Engaging in surreptitious and unexpected collection or use of biometric information.***
- ***Failing to evaluate the practices and capabilities of third parties.***

- ***Failing to provide appropriate training for employees or contractors.***
- ***Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or uses in connection with biometric information.***

Takeaways

In many ways, this Policy Statement follows the approach that the FTC has taken in privacy and security cases for decades. However, the Policy Statement does attempt to impose substantive requirements on companies (i.e., risk assessments) and further evidences the FTC's commitment to leveraging Section 5 as a disparate impact antidiscrimination statute. The Commission is clear that companies' risk assessments should consider whether any algorithms or technical components of the system have been tested for disparate impact. The strong implication is that companies must not use algorithms or technology that have not been tested for disparate impact. Commissioner Bedoya, in his statement at the Opening Meeting, emphasized his belief that companies cannot use technology until they have thought about how bias could affect consumers and proactively address such harms.

The Statement also provides insight into how the Commission will evaluate the reasonableness of companies' use of biometric data. Under Section 5 of the FTC Act, in order for the Commission to find a practice unfair, it must determine that it causes or is likely to cause substantial injury to consumers, that is not reasonably avoidable by consumers, and is not outweighed by any countervailing benefits to consumers or competition. In the privacy and data security space, the FTC's unfairness determination has been guided by an assessment of whether a company's overall practices were reasonable. Traditionally, the FTC has steered away from bringing cases that ultimately require the FTC to argue that a business made a decision that, in hindsight, was not optimal. In the Policy Statement, the FTC states that if it feels that companies' employing biometric information in their technology could have used a "less risky alternative," it will weigh that more heavily against any arguments that the technology was more convenient, efficient, or profitable. The FTC seems skeptical that companies could present evidence of benefits to consumers or competition that could outweigh what it views as serious risk of injury to consumers.

The Policy Statement is another reminder that regulators are focused on the use and collection of sensitive data, and businesses collecting or using biometric data should review their practices to determine whether they comport with this latest guidance.