Updates
June 09, 2023
FTC Issues Policy Statement Regarding Biometric Information

The Federal Trade Commission (FTC) issued a policy statement on May 18, 2023, addressing concerns relating to the collection and use of biometric information. The Biometrics Policy Statement, which the FTC's Commissioners voted 3-0 to issue, outlines practices related to biometric information that the FTC views as violations or will take into account when evaluating possible violations of the prohibition against unfair or deceptive acts and practices in Section 5 of the FTC Act.

Biometric Information

The Biometrics Policy Statement defines "biometric information" broadly 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." According to the FTC, this includes "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)," as well as "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 has been derived."

Notably, the FTC's definition of "biometric information" includes photographs of a person's face, genetic information, and "characteristic movements or gestures," which are data types not commonly encompassed within legal definitions of "biometric" data under other bodies of law.

Citing a "proliferation of biometric information technologies," the Biometrics Policy Statement highlights the "new and increasing risks associated with the collection and use of biometric information," including the

possibility that this information could be used to produce "counterfeit videos or voice recordings (so-called 'deepfakes')" and potential unauthorized use of biometric data to access devices by malicious actors. The Biometrics Policy Statement also highlights that technologies using biometric data, including facial recognition technology, may lead to discriminatory outcomes for certain demographic groups.

The FTC's Statutory Basis for Regulating Biometric Information

The FTC does not enforce a law or regulation specifically addressing biometric information, and at this time, there is no comprehensive federal law specifically addressing the collection and use of biometric information by commercial entities. As the Biometrics Policy Statement acknowledges, several state and local jurisdictions have adopted biometric information privacy laws. But, the FTC enforces Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices. The Biometrics Policy Statement makes clear that the FTC views Section 5 as a tool that enables it to regulate the collection and use of biometric information.

In the Biometrics Policy Statement, the FTC also opines that various other laws and regulations at the federal level that it enforces may govern biometric information as well, including the Children's Online Privacy Protection Rule, 15 U.S.C. § 6501, *et seq.*; the Health Breach Notification rule, 16 C.F.R. Part 318; and the Gramm-Leach-Blilely Act's Safeguards Rule, 16 C.F.R. Part 314, and Regulation P, 12 C.F.R. Part 1016.

Biometric Information Practices the FTC Will Scrutinize

In the Biometrics Policy Statement, the FTC lists specific examples of business practices relating to biometric information that it will scrutinize under Section 5.

1. Deceptive Practices

The Biometrics Policy Statement first addresses potentially deceptive claims relating to the collection and use of biometric information and related technologies:

- **Deceptive marketing claims relating to biometric information technologies.** The Biometrics Policy Statement warns that "false or unsubstantiated claims relating to the validity, reliability, performance, fairness, or efficacy of technologies using biometric information" may be deemed to violate the FTC Act. The FTC appears to be particularly concerned about claims relating to real-world performance of biometric information technologies that rely on testing or data that do not replicate real-world conditions.
- **Deceptive statements about the collection and use of biometric information.** The FTC also cautioned that false or misleading statements about "the extent to which [companies] collect or use biometric information or whether or how they implement technologies using biometric information" may also violate the FTC Act. In particular, the Biometrics Policy Statement warns against "telling half-truths," such as "mak[ing] an affirmative statement about some purposes for which [they] will use biometric information but fail[ing] to disclose other material uses of the information."

2. Unfair Acts

Importantly, the Biometrics Policy Statement also addresses potentially "unfair" acts relating to the collection and use of biometric information and related technologies. The legal standard for whether a practice is "unfair" is whether it causes or is likely to cause substantial injury to consumers that is (1) not reasonably avoidable by consumers themselves and (2) not outweighed by the countervailing benefits to consumers or competition. This is almost inherently a contextual determination requiring consideration of the full set of relevant facts and circumstances surrounding a practice. For the most part, rather than list specific practices as unfair, the Biometrics Policy Statement advises that the FTC "will take into account factors including, but not limited to, the following":

- **Whether the business failed to assess foreseeable harms before collecting biometric information and/or failed to promptly address known or foreseeable risks.** The Biometrics Policy Statement encourages businesses to conduct a "holistic assessment" to identify and address potential risks associated with biometric technology *before* they deploy the technology or collect consumers' biometric information. This assessment should include the context in which the collection or use will occur, the extent to which biometric information technologies have been tested, whether the relevant technology "leads to or contributes to outcomes that disproportionately harm particular demographics of consumers," as well as whether any algorithmic portions of the technology "have been specifically tested for differential performance across demographic groups—including intersectionally." Relatedly, the Biometrics Policy Statement says businesses should seek to identify and implement readily available tools for reducing or eliminating risks, including measures to address the risk of consumer injury from technologies that may lead to bias or error.
- **Whether the business failed to evaluate third parties' practices and capabilities.** The Biometrics Policy Statement emphasizes that businesses should evaluate third parties that may be given access to biometric information, including affiliates, vendors, and end users. According to the FTC, this should include seeking contractual agreements requiring third parties to take appropriate steps to minimize risk to consumers, where applicable. Additionally, the FTC states that businesses "should also go beyond contractual measures to oversee third parties and ensure they are meeting those requirements," including potentially implementing "organizational and technical measures . . . to supervise, monitor or audit" compliance.
- **Whether the business failed to provide appropriate training for employees and contractors.** The Biometrics Policy Statement states that companies should appropriately train employees and contractors whose job duties involve interacting with biometric information or related technologies.
- **Whether the business failed to monitor biometric technologies the business develops, sells, or uses.** The Biometrics Policy Statement also states that companies should monitor biometric technologies that they develop, use, sell, or otherwise provide to others to ensure that those technologies function as anticipated and are not likely to harm consumers.
- **Per se unfair practices?** The Biometrics Policy Statement states that the following practices may be "unfair in and of [themselves]," which suggests there may be a high bar to convincing the FTC that evidence of minimal extent or type or likelihood of injury, reasonable avoidability, and/or countervailing benefits renders a practice falling within this list lawful:
    - "[Using] or facilitat[ing] the use of" biometric information "to surreptitiously identify or track a consumer in a manner that exposes the consumer to risks such as stalking, exposure to stigma, reputational harm, or extreme emotional distress."
    - Failing to "clearly and conspicuously disclose the collection and use of biometric information."
    - Failing to have a "mechanism for accepting and addressing consumer complaints and disputes related to ... use of biometric information technologies."

What's Next?

Policy statements tend to portend enforcement activity, and the FTC may conduct investigations or bring cases relating to the practices outlined in the Biometrics Policy Statement. Additionally, as we covered in August 2022, the FTC asked about the collection and use of biometric data in its advance notice of proposed rulemaking on "commercial surveillance and data security" (ANPRM), including a question asking if the FTC should "consider limiting commercial surveillance practices that use or facilitate the use of facial recognition, fingerprinting, or other biometric technologies." No rule proposals have emerged from the ANPRM to this point, but proposals could come in that process for regulations on the collection and use of biometric information.

Companies that collect or process biometric information should consider what steps they can take in light of the Biometrics Policy Statement. For example, many of the factors listed in the statement as relevant to whether a given practice is deceptive or unfair can be addressed or mitigated in advance through proactive compliance measures, which may be similar to but potentially slightly different from practices a company may already employ to comply with state biometrics laws or as part of a comprehensive privacy and data security program.

Authors

Explore more in

Privacy & Security Technology Transactions & Privacy Law Digital Media & Entertainment, Gaming & Sports

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law