
FTC Signals Increased Scrutiny of Biometric Technologies

MAY 22, 2023

On May 18, the Federal Trade Commission (FTC) issued a [policy statement](#) warning about the increased use of consumers' biometric information and related marketing of technologies that use biometric information. The agency notes that these technologies raise considerable consumer privacy and data security concerns, as well as the potential for bias and discrimination.

This guidance by the FTC is the latest indication that the agency is willing to use all the tools available at its disposal to protect what it deems to be more sensitive or higher-risk information about consumers. Similar to the FTC's approach to protecting consumer health information over the past couple of years, the agency has put forward an extremely expansive definition of what constitutes "biometrics," indicating that the agency has its own approach to the issue that will not necessarily be influenced by how state laws or other regulators have addressed it. Additionally, the FTC specifically enumerates "unfair" acts or practices relating to the processing of biometrics (such as engaging in the "unexpected" collection of biometrics).

We note that one of the potential "unfair" acts or practices that the FTC identified in this guidance as a potential violation of the FTC Act is a business's failure to identify "foreseeable risks" related to the processing of biometrics. While the FTC statement does not go as far as explicitly requiring data protection assessments, businesses that fail to do risk assessments around their use of biometric information will have a difficult time showing that they did any meaningful assessment of the "foreseeable harms" in relation to their biometric data processing (in a potential FTC enforcement action). This policy statement is another illustration of the FTC taking an expansive view of its unfairness authority under Section 5 of the FTC Act (as it has done recently [for health information](#)), as well as its continued emphasis on substantive data limitations.

In addition, the FTC stresses that a practice need not be equally likely to harm all consumers to be considered unfair, and that the FTC will consider practices from the perspective of any population of consumers that is particularly at risk of harm. The broad language here suggests that consumer harm need not be to a recognized protected class of consumers. Therefore, businesses should carefully assess all potential consumer injury risks associated with biometric technologies when conducting risk assessments.

The policy statement makes clear that the FTC will likely place heightened scrutiny on businesses

employing biometric technologies and making marketing claims related to them. Businesses that use biometric information should carefully review the policy statement to understand the types of data practices that the FTC will find potentially problematic, as this policy statement is a clear indication of the types of issues that the FTC will be investigating.

In the rest of this post, we identify and elaborate upon the key takeaways from the FTC's guidance. We are happy to answer any questions you may have. You can also stay on top of our updates by subscribing to the [WilmerHale Privacy and Cybersecurity Blog](#).

Broad Definition of Biometric Information

In the policy statement, the agency adopts an expansive definition of biometrics. Under the FTC's definition, biometric information is "data that depict or describe physical, biological, or behavioral traits, characteristics, or measurements of or relating to an identified or identifiable person's body." Examples of biometric data include, but are 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." The FTC further details that biometric data includes "data derived from such depictions, images, descriptions, or recording to the extent that it would be reasonably possible to identify the person from whose information the data has been derived."

The agency also states that, although in some contexts, "biometrics" or "biometric technologies" refer to technologies used to identify individuals, the FTC uses "biometric information technologies" to refer broadly to all technologies that use or purport to use biometric information for any purpose. Compared to how biometrics are defined under other laws, this is an extremely expansive definition. For example, the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), defines "biometric information" as "an individual's physiological, biological or behavioral characteristics... that can be used, singly or in combination with each other or with other identifying data, to establish individual identity" (emphasis added). The FTC's definition is even broader than the definition in Illinois's Biometric Information Privacy Act (BIPA)—perhaps the most well-known of the state biometric privacy laws—because the FTC's definition of biometric information explicitly includes "derivative data" to the extent that it would be reasonably feasible to identify the person from whose information the data has been derived from that information.

Risks of Biometric Information

The FTC's policy statement notes multiple risks associated with the collection and use of biometric information, presumably as a way of bolstering its case for consumer harm. For instance, the FTC notes that biometric information can be used to produce deepfakes and that large databases of biometric information have the potential to be used by malicious actors for unlawful purposes. Furthermore, when biometric information is linked to consumers' location information, the FTC states that it could reveal sensitive personal information such as healthcare data or an individual's attendance at religious or political events.

The agency also recognizes the bias and discrimination risks inherent in biometric technologies. For example, the FTC states that facial recognition algorithms produce more false positive matches

for images of non-Europeans, women, and in the elderly and children. Therefore, the FTC takes the position that biometric technologies might perpetrate biases and discrimination for certain groups.

Potential Unfair or Deceptive Acts or Practices Related to Biometrics

The FTC outlines a list of practices relating to biometric information that fall under its FTC Act Section 5 authority of enforcing deceptive and unfair practices. The agency highlights that it will conduct “a holistic assessment” of businesses’ relevant practices in determining violations, but specifically notes that it will draw on lessons learned from past privacy and data security matters.

Deceptive practices

1. False or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information – Businesses should not make unsubstantiated marketing claims that technologies are unbiased if such claims cannot be proven. Businesses should also avoid making false claims about real-world accuracy of biometric information technologies when underlying tests or audits do not mirror real-world conditions. The FTC also cautions businesses against making unsubstantiated claims about whether technologies can yield particular outcomes, such as reductions in rates of theft or the elimination of bias in hiring.
2. Deceptive statements about the collection and use of biometric information – Businesses should not make false statements about the extent to which they collect or use biometric information. The agency will also scrutinize “half-truths,” which are misleading if businesses make affirmative statements about some uses of biometric information but do not disclose other material uses.

Unfair practices

1. Inadequate privacy and data security measures – Businesses should ensure that any biometric data they collect is protected from unauthorized access, including external cybersecurity attacks and internal unauthorized access from employees, contractors, or service providers.
2. Failing to assess foreseeable harms to consumers before collection biometric information – Businesses should conduct a comprehensive evaluation of potential risks posed by collecting biometric data before doing so. These risk assessments should consider the context of the data collection and data use, along with the extent to which biometric information technologies have been tested by the business itself or by third parties. The FTC also cautions businesses from presuming without evidence that the involvement of human operators by default mitigates risk to consumers.
3. Failing to promptly address known or foreseeable risks – If there is evidence that a biometric technology is susceptible to certain types of errors or biases, businesses should be especially cautious of potential consumer injury because of these risks. Businesses should also employ technical safeguards, such as timely updates on systems that capture, process, or store biometric information to ensure safe operation of these systems.
4. Engaging in surreptitious and unexpected collection or use of biometric information –

Conduct can be unfair and unlawful if businesses use biometric information to surreptitiously identify or track consumers in a manner that exposes consumers to risks such as stalking, reputational harm, or extreme emotional distress. Businesses should clearly and conspicuously disclose the collection and use of biometric information. Businesses should also put in place mechanisms to address consumer complaints because the lack of such measures can compound the risk of consumer injury.

5. Failing to provide appropriate training for employees and contractors – All employees whose job duties include interaction with biometric information or technologies should receive proper training on how to use and protect such information.
6. Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or uses in connection with biometric information – Businesses should ensure that technologies are not only functioning as designed, but also that biometric technologies are being used as intended. Businesses should regularly monitor whether the use of technology is likely to harm customers.

Authors



Kirk J. Nahra

PARTNER

Co-Chair, Artificial
Intelligence Practice

Co-Chair, Cybersecurity
and Privacy Practice

✉ kirk.nahra@wilmerhale.com

☎ +1 202 663 6128



Arianna Evers

PARTNER

✉ arianna.evers@wilmerhale.com

☎ +1 202 663 6122



Ali A. Jessani

COUNSEL

✉ ali.jessani@wilmerhale.com

☎ +1 202 663 6105