Staying Ahead of the Curve: Understanding and Adapting use of Biometrics in the Wake of the Federal Trade Commission's Guidance

Oct 21, 2025

Categories:

Publications

Authors:

John T. Wolak
Julia E. Browning
Ravipal Singh

Use of biometric data has become an integral part of everyday life: It unlocks your phone with face-ID or voice recognition; it verifies your identity at work or the gym with a fingerprint or palm scan; it allows access to secure buildings, areas, and files; and it expedites your clearance at airport security for both domestic and international flights. As the commercial uses of biometric data increase, so do concerns about consumer privacy, data security, potential for bias and discrimination, and a consumer's control of this uniquely personal identifying information.

In response to these concerns, regulators and lawmakers have increasingly been focused on biometric data privacy and the complex web of inter-related issues that arise with the use of consumer biometric information. Several states and municipalities have adopted statutes or regulations specifically establishing requirements for the collection and use of biometric data, while other states have included biometric information in the "personal data" subject to the respective state's omnibus privacy statute. At this juncture, there is no federal statute or regulation that directly addresses the commercial use of biometric data. However, the Federal Trade Commission (FTC) has emerged as the leading federal agency in this area, having issued a formal policy statement and undertaken enforcement actions confirming that it is committed to combating unfair or deceptive practices in connection with the collection and use of consumers' biometric information and the marketing and use of biometric information technologies.

This overview discusses the FTC's policy statement and past enforcement actions relating to collection and use of biometric data, identifies other federal agencies that have issued regulations relating to use of biometrics and certain state laws applicable to biometric information, and provides action items for compliance

efforts and best practices that will assist businesses attempting to align with the FTC's proscriptions. A subsequent overview will cover in greater detail the various state statutes and regulations applicable to the collection and use of biometric data from residents of the subject state.

I. The Federal Trade Commission Policy Statement

On May 18, 2023, the FTC issued the "Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act" (the "Policy Statement") setting forth a non-exhaustive list of practices it will scrutinize to determine whether companies collecting and using biometric information or marketing biometric information technologies are complying with Section 5 of the Federal Trade Commission Act (the "Act").

At the outset, the FTC broadly defined "biometric data" 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" including, but 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)." The FTC continued that "[b]iometric 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." It is important to note that the FTC's definition of biometric information is typically broader than most state and municipal laws, which may trigger compliance obligations with FTC requirements that otherwise do not exist under state or local laws.

With this broad definition as its base, the FTC identifies a number of risks arising from the collection and use of biometric information for both consumers and businesses alike, such as:

• producing counterfeit videos or voice recordings (so-called "deepfakes");

• developing large databases of biometric information that may be targeted by malicious actors for use in other illicit activities;

• identifying consumers in certain locations, which could reveal sensitive personal information like accessing healthcare, or religious, political, or union activities;

• creating false or inaccurate results (*e.g.,* a false positive could result in an individual being wrongly accused of a crime; a false negative could result in an individual being denied access to their own bank account); and

• enabling discriminatory outcomes because the technology may perform differently across different demographic groups.

In light of these potential risks, the FTC set out a non-exhaustive list of prohibited practices under Section 5 of the act with respect to the collection and use of biometric information in two primary areas – deceptive practices and unfair practices:

• ***Deceptive Practices,*** which include:

• false or unsubstantiated marketing claims relating to the validity, reliability, accuracy, performance, fairness, or efficacy of technologies using biometric information; and

• deceptive statements about the collection and use of biometric information.

• ***Unfair Practices,*** which include a practice that:

• causes or is likely to cause substantial injury to consumers;

• cannot be reasonably avoided by consumers or occurs surreptitiously or without meaningful consumer choice; or

• is not outweighed by benefits to consumers.

To determine whether a business collecting and using biometric information or biometric information technology has violated Section 5 of the Act, the FTC will assess and evaluate the business's practices regarding the collection, use, storage, and claims for processing biometric information, which include the following factors:

• Failure to assess foreseeable harms before deploying biometric technologies.

• Prior to collecting consumers' biometric information, has the business conducted a holistic assessment of the potential risks to consumers associated with the collection and use, including:

i. the context and purpose for the collection or use;

ii. the extent to which the specific biometric information technologies have been tested by the business or a third party;

iii. whether the testing mirrors real-world implementation and use;

iv. the appropriate role of human operators and their effectiveness in mitigating risks to consumers; and

v. the potential for outcomes that may give rise to disproportionate harm to particular demographics of consumers?

• Failure to promptly address known or foreseeable risks.

• Has the business taken appropriate steps to reduce or eliminate risks that could lead to consumer injury, including implementing organizational measures (like policies and procedures), as well as technical measures (like updates or alternatives to existing systems and processes)?

• Surreptitious and unexpected collection of biometric information.

• Is the business using biometric information or biometric information technology to surreptitiously identify or track a consumer in a manner that exposes the consumer to potential stigma, reputational harm, or emotional distress?

• Has the business clearly and conspicuously disclosed the collection and use of biometric information to allow actual consumer choice about such collection and use?

• Failure to evaluate the practices and capabilities of third parties.

• Has the business obtained appropriate assurances and contractual agreements from third parties who can access biometric information to take appropriate steps to minimize risks to consumers?

• Does the business monitor third parties to ensure they are meeting those requirements and not putting consumers at risk?

• Failure to provide appropriate training for employees and contractors.

• Does the business provide – and require third-party contractors to provide – regular comprehensive training for all individuals whose job duties involve biometric information or biometric information technologies?

• Failure to conduct ongoing monitoring of technologies that the business develops, offers, or uses in connection with biometric information.

• Does the business complete regular monitoring of its technologies – including technologies it uses in regular operations – to ensure that the technologies are functioning as anticipated, are being used and are operating as intended, and that such use and operations are not likely to harm consumers?

II. FTC Enforcement

The FTC has had two notable enforcement actions related to the misuse of biometric information. In its first-ever enforcement action related to the use of biometric technology, the FTC alleged that Everalbum, a photo development application, falsely represented that it would not use facial recognition technology without the consumer's affirmative consent, and misled users by claiming that it would delete photos and videos once the user's account was deactivated. In reality, Everalbum retained the consumer's biometric data indefinitely. As part of the settlement with the FTC, Everalbum agreed to obtain express consent from users before using facial recognition, delete all biometric data from deactivated accounts, and refrain from using biometric data in any future software without first obtaining consumer consent.

In a separate action against Rite Aid, the FTC alleged that Rite Aid deployed biometric technology without implementing reasonable safeguards. Rite Aid used facial recognition in retail locations to identify customers that it had previously deemed likely to engage in shoplifting or other criminal behavior. In numerous instances, the match alerts from the system Rite Aid was using were false positives, and therefore the FTC found that Rite Aid failed to consider or address foreseeable harms to consumers, failed to test

the technology's accuracy, failed to enforce image quality standards, and failed to take reasonable steps to train and oversee the employees charged with operating the technology in Rite Aid stores.

III. Other Regulatory Actions by Federal Agencies

In addition to the FTC, the Federal Communications Commission (FCC), the Consumer Financial Protection Bureau (CFPB), and the Department of Justice (DOJ) have all adopted regulations related to the collection and use of biometric information. For example:

• On Dec. 13, 2023, the FCC adopted an order, which expanded the scope of the data breach notification rules applicable to telecommunications carriers and interconnected VoIP providers by, *inter alia*, broadening the definition of "covered data" to include "unique biometric, genetic, or medical data."

• On Oct. 24, 2024, the CFPB issued guidance to protect workers from unchecked digital tracking and opaque decision-making systems. Specifically, the guidance warns that companies using third-party consumer reports — including background dossiers and surveillance-based, "black box" AI or algorithmic scores about their workers — must follow Fair Credit Reporting Act (FCRA) rules by obtaining worker consent, providing transparency about data used in adverse decisions, and allowing workers to dispute inaccurate information.

• In Dec. 2024, the Department of Homeland Security, DOJ, and White House Office of Science and Technology Policy submitted a "Biometric Technology Report" to provide a public overview of how these agencies are using biometric technologies, particularly in the law enforcement space.

IV. State and Local Regulatory Action

Currently, there are four states with comprehensive biometric privacy laws and regulations:

• ***Colorado***: Colorado Privacy Act, Colo. Rev. Stat. Ann. § 6-1-1314;

• ***Illinois***: Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 *et seq.;*

• ***Texas***: Capture or Use of Biometric Identifier Act ("CUBI"), Tex. Bus. & Com. Code Ann. § 503.001; and

• ***Washington***: Washington Consumer Protection Act, Wash. Rev. Code §§ 19.375.010 *et seq*. and the 2023 My Health, My Data Act.

In addition to these comprehensive statutes, there are a number of state and city-specific regulations with respect to the use of biometric information in public places or related to employment, including:

• ***New York***: City of New York Administrative Code, Title 22, Chapter 12 and N.Y. Lab. Law § 201-aA

• ***Oregon***: Portland City Code, Title 34- Digital Justice, Chapters 34.10.010-34.10-050

• ***Maryland***: Labor and Employment Code § 3-717

Finally, most states that have enacted omnibus data privacy laws include biometric information within the scope of "personal data" that is subject to collection, use processing, and storage requirements.

V. Best Practices for Implementation and Compliance

As businesses look to the use of biometric information and related technologies to enhance and improve daily operations, careful consideration must be given to developing appropriate practices, policies, and procedures for the collection, use, and storage of biometric information in order to align with the FTC's proscriptions. Businesses should consider the following when deciding to collect, use, or store biometric information or implement biometric information technology, as well as drafting policies for such uses:

• Establish a legitimate, operations-based reason for the collection and use of biometric information;

• Ensure the accuracy and completeness of the disclosures and claims to be made with respect to the use and collection of biometric information and biometric information technologies;

• Develop appropriate mechanisms for making consumer disclosures detailing the circumstances of collection, use, and storage;

• Obtain appropriate consent for the disclosed purposes of collection, use, and storage;

• Continually assess whether the use of biometric information or biometric information technologies causes or is likely to cause any foreseeable risks to consumers, actual consumer injury, or any disproportionate harm to particular demographics;

• Establish clear policies, procedures, and practices for collection, use, and storage of biometric information that reduces or eliminates the risks that could lead to consumer injury and (if necessary) incorporates appropriate enhancements for particularly sensitive uses like hiring, surveillance, or decisions that may have legally significant consequences;

• Complete comprehensive and regular risk assessments of relevant biometric information processing and practices, which should draw from lessons learned in similar situations such as in the privacy and data security context;

• Implement reasonable privacy and data security measures to ensure that any biometric information that is collected or maintained is protected from unauthorized (internal and external) access;

• Regularly train employees who are responsible for handling or processing biometric information on best practices and how to properly manage biometric information;

• Ensure that retention policies for biometric information are closely tied to legitimate business purposes and avoid overbroad or indefinite retention of biometric information; and

• Complete regular monitoring of third-party vendors to ensure ongoing compliance with contractual and operational requirements and safeguards.

Finally, because the potential uses of biometric information span across virtually all industries (*e.g.*, healthcare, financial services, travel, law enforcement, etc.), it is critical that businesses also review industry-specific standards and guidelines to ensure that any biometric information policies and practices are up to date and appropriate to meet any other requirements and compliance

obligations.

VI. What's Next?

Similar to the data privacy space, regulation and enforcement related to the collection, use, and storage of biometric information is ever-changing, particularly as businesses find new ways to implement this technology and bad actors find new ways to exploit it. Looking ahead, the FTC's enforcement activity is likely to expand in response to the rise of AI and the continued expansion of biometric applications and use. For example, the bipartisan "Take It Down Act" enacted on May 19, 2025, does not directly regulate collection or use of biometric information, but it empowers the FTC to protect individuals against "deepfake" abuses and hold platforms accountable for failing to remove non-consensual AI-generated content. At the same time, there have been recent high-profile incidents involving voice cloning and "deepfake" technology. These developments point toward a future where the FTC continues to leverage its Section 5 authority and initiatives to address misuse and abuse of biometric information and AI technology. While it is impossible to predict what will come next, closely monitoring pending legislation, using lessons learned from the evolution of data privacy laws, and following best practices designed to reduce or eliminate the risk of consumer injury will enable businesses to stay ahead of the curve.

FBT Gibbons