PUBLICATION

FTC Rite Aid Settlement Offers Key Lessons for Mitigating Risk When Deploying Biometrics or AI Tools

Authors: David J. Oberly
December 29, 2023

On December 19, 2023, the Federal Trade Commission (FTC or Commission) announced its settlement of an enforcement action against retail pharmacy chain Rite Aid over alleged violations of Section 5 of the FTC Act (Section 5) stemming from its use of facial biometric technology. The Rite Aid matter is a critical development for all companies that offer or utilize biometric or artificial intelligence (AI) tools today, and it provides a number of key takeaways for managing the significantly increased risks that now exist in connection with heightened FTC scrutiny over the commercial use of this advanced technology.

Background

According to the FTC, Rite Aid used facial biometrics at its retail locations to identify and remove individuals "likely to engage in criminal activity from" its stores. Rite Aid's biometric security technology operated by pushing alerts to employees that a "person of interest" had been identified as entering their store, after which time notified employees would take action, including through increased human monitoring and reporting criminal activity to the police. In many instances, these alerts were purportedly the result of "false positive" matches incorrectly identifying someone as having been entered into Rite Aid's database as a so-called person of interest.

In its Complaint, the FTC alleged that Rite Aid's use of facial biometrics constituted unfair acts or practices in violation of Section 5 as a result of the company's failure to take reasonable steps to address the risk that its deployment of such technology was likely to result in harm to consumers, particularly with respect to false positive match results – which presented an especially acute risk to minority customers.

In addition, the Commission also asserted a separate Section 5 claim in connection with Rite Aid's purported failure to comply with a 2010 order issued by the FTC, which had required, among other things, that Rite Aid: (1) exercise reasonable diligence in selecting and retaining service providers that were capable of appropriately safeguarding its personal data; (2) obtain contractual assurances from its service providers regarding the security of personal data maintained by those vendors; and (3) implement and maintain a written information security program.

Settlement Terms

To resolve the matter, Rite Aid entered into a Stipulated Order with the FTC that imposes the following key requirements and restrictions:

- **Blanket Ban on Use of Facial Biometrics**. Rite Aid is prohibited from using any type of facial biometrics for a period of five years.
- **Requirements and Restrictions on Use of *All* Biometric-Powered Tools**. Rite Aid must satisfy a range of requirements pertaining to its collection and use of biometric data before deploying or using any type of biometric technology, including: (1) a biometric system monitoring program (discussed in

more detail below); (2) data retention and destruction schedules and guidelines; (3) individualized and public notice/disclosures; and (4) consumer complaint procedures.

- **Biometric System Monitoring Program**. Rite Aid must implement a biometric system monitoring program that includes: (1) extensive pre-deployment risk and impact assessment requirements; (2) regular post-deployment assessments to evaluate the ongoing effectiveness of its program (and remediation of any consumer risks identified through those periodic assessments); and (3) implementation of a number of safeguards to address and control for identified consumer risks, including: (a) testing and monitoring of biometric system accuracy; (b) employee training and oversight; (c) written biometric data quality standards; (d) service provider diligence and contract requirements; and (e) recordkeeping regarding actions taken based on biometric system outputs.
- **Data and Algorithmic Disgorgement**. Rite Aid must delete all *data*, *models*, *and algorithms* developed or derived from its improper use of facial biometrics. It must also notify all vendors and other third parties that performed services on the company's behalf to permanently destroy all data, models, algorithms, and *biometric data* received from Rite Aid in connection with its use of facial biometrics.
- **Information Security Program and Third-Party Assessments**. Separate from its biometric system monitoring program, Rite Aid must implement a broader information security program to protect the security, confidentiality, and integrity of personal data collected and possessed by the company or its service providers, and have its program validated through regular assessments conducted by an independent third-party assessor.

Analysis and Takeaways

The Rite Aid action is noteworthy for all companies that develop, use, or intend to use biometrics or AI in their operations, and it provides several valuable lessons and takeaways that can be leveraged to reduce the risk of regulatory scrutiny, while also offering key insight into how the FTC is actively thinking about major biometrics and AI issues. Moreover, the action also highlights the specific aspects and elements of biometrics and AI tools, as well as how those tools are operated, that the Commission is likely to focus on with greater scrutiny in future investigations and enforcement actions.

Taken together, companies and their senior leadership can utilize what the FTC has identified as its major concerns and take proactive measures to address these issues, thereby mitigating the rapidly rising legal risks that organizations now face in terms of potential FTC liability in connection with the use of these advanced tools.

From a broader perspective, the Rite Aid action serves as an unequivocal warning that the FTC will continue to make both biometrics and AI primary focus areas for the Commission for the foreseeable future, which should prompt all businesses that develop or utilize biometric or AI technology to devote the necessary time, effort, and resources to address these increasing liability exposure risks posed by the FTC. At the same time, building out a comprehensive biometrics/AI governance program now will give organizations a head start on managing the associated legal risks that will soon materialize in the near future when additional laws governing the deployment of these tools are inevitably enacted – sooner than later – which will ultimately develop into a ubiquitous part of the legal landscape.

What to Do Now: Practical Compliance Tips

Beyond offering an informative illustration of what not to do when deploying biometric or AI tools, the Rite Aid matter highlights a number of specific practices that the FTC will expect companies to have in place when scrutinizing the commercial use of this technology for potential Section 5 noncompliance moving forward.

Notably, in his written remarks regarding the matter, Commissioner Alvaro Bedoya highlighted that the Rite Aid settlement "offers a strong baseline for what [a biometrics or AI compliance] program should look like."

Companies should give consideration to implementing the following to enhance their compliance programs:

- **Biometric System Monitoring Program**. Follow the blueprint articulated by the FTC relating to biometric system monitoring programs. Such programs should encompass three primary components: (1) mandatory risk and impact assessments to be completed before the deployment of new biometrics tools, as well as before any major modifications to current biometric data processing activities are made; (2) regular, ongoing assessments for continued monitoring and evaluation; and (3) tailored controls for addressing the risks identified during the organization's biometric assessments. Such programs should also include the following controls: (1) accuracy testing mechanisms; (2) data/image quality controls; (3) employee training and monitoring; and (4) recordkeeping protocols for documenting actions taken based on system outputs.
- **Notice**. Implement mechanisms to provide notice and promote transparency with respect to biometrics systems, including: (1) individualized notice to data subjects before: (a) biometric data is collected; and (b) taking adverse action in connection with system outputs that could result in physical, financial, or reputational harm to consumers; (2) general notice on each website where biometric data is collected online; and (3) clear and conspicuous signage in each physical location where biometric systems are operated.
- **Data Retention/Destruction**. Implement and thereafter follow a set biometric data retention schedule and guidelines for permanently deleting biometric data.
- **Consumer Complaint Mechanism**. Implement at least one method for consumers to submit complaints regarding the outputs produced by biometric systems (as well as more general concerns relating to organizational biometric data processing activities), along with a process and protocols for investigating and responding to consumer complaints.
- **Information Security Program**. Independent of any biometric system monitoring program, implement an information security program to protect the security, confidentiality, and integrity of biometric data – as well as all other forms of personal data – collected and maintained by the organization and its service providers. Programs should also be regularly validated through third-party assessments.

For more information or assistance with biometrics or AI matters, please contact David J. Oberly or a member of Baker Donelson's Biometrics or AI Teams.