Kilpatrick

January 4, 2024

Companies Deploying Facial Recognition Continue to be Watched; Rite Aid Banned from Using AI Facial Recognition

by Tatum Andres

On December 19, 2023, Rite Aid Corporation (Rite Aid) agreed to settle Federal Trade Commission (FTC) charges that it failed to take reasonable measures to prevent harm to consumers from its use of facial recognition technology, which amounted to an unfair practice under Section 5 of the FTC Act.

Specifically, the FTC's complaint alleged that Rite Aid obtained facial recognition technology from two third-party vendors and subsequently directed these vendors to create a database of images of individuals whom Rite Aid considered "persons of interest." Persons of interest included individuals who had previously engaged in actual or attempted criminal activity at a Rite Aid location or whom Rite Aid obtained "BOLO" ("Be On the Look Out") information about the individual from law enforcement.

Cameras installed in Rite Aid's retail pharmacy locations, that used facial recognition technology, would capture (or attempt to capture) images of all consumers as they entered or moved through the stores. Rite Aid's facial recognition technology would then compare the captured images to the images in Rite Aid's person of interest database to determine whether the captured image was a match. If the employee believed the match to be accurate, Rite Aid instructed employees to approach the person, ask them to leave, and, if the person refused, call the police. However, Rite Aid's facial recognition technology generated numerous false positive facial recognition match alerts.

"Rite Aid's reckless use of facial surveillance systems left its customers facing humiliation and other harms, and its order violations put consumers' sensitive information at risk," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "[This] groundbreaking [settlement] order makes clear that the Commission will be vigilant in protecting the public from unfair biometric surveillance and unfair data security practices." Notably, earlier this year, the FTC issued a policy statement serving as a warning that the increasing use of consumers' biometric information and related technologies, including those powered by machine learning, raises significant consumer privacy and data security concerns and the potential for bias and discrimination. The policy statement also notes that it will consider several factors in determining whether a business's use of biometric information or biometric information technology would violate the FTC Act including:

- Failing to assess foreseeable harms to consumers before collecting biometric information;

- Failing to promptly address known or foreseeable risks and identify and implement tools for reducing or eliminating those risks;
- Engaging in surreptitious and unexpected collection or use of biometric information;
- Failing to evaluate the practices and capabilities of third parties, including affiliates, vendors, and end users, who will be given access to consumers' biometric information or will be charged with operating biometric information technologies;
- Failing to provide appropriate training for employees and contractors whose job duties involve interacting with biometric information or technologies that use such information; and
- Failing to conduct ongoing monitoring of technologies that the business develops, offers for sale, or uses, in connection with biometric information to ensure that the technologies are functioning as anticipated and that the technologies are not likely to harm consumers.

According to the FTC's complaint, Rite Aid failed to use appropriate procedures in the following areas:

- Failing to consider and address risks to consumers, including increased misidentification risk based on race or gender;
- Failing to test or assess accuracy before deployment;
- Failing to enforce image quality controls;
- Failing to train and oversee employees; and
- Failing to monitor, assess, or test the accuracy of results.

The FTC continues to require companies to delete ill-gotten data (and the technology built using such data) in response to privacy violations. The FTC settlement order imposes a ban on Rite Aid's use of A.I. facial recognition technology for five years. Among other actions, it also requires the company to destroy all photos and videos of consumers used or collected in connection with the operation of a facial recognition or analysis system prior to the effective date of the order. Rite Aid must also instruct all third parties that received biometrics to destroy all models or algorithms developed with the wrongly collected facial images. It is important that companies, employing facial recognition technology, work with vendors to ensure that there are procedures in place for deleting information after some period has elapsed. In-house counsel should also communicate the risk of algorithmic disgorgement to business stakeholders when counseling business leaders on the risks associated with machine learning and similar product development activities.

Rite Aid's case serves as a reminder of increasing scrutiny surrounding the use of A.I., facial recognition, related machine learning, and the importance of ethical practices in deploying advanced technologies. Notably, following the proposed stipulated order against Rite Aid, FTC Commissioner, Alvaro Bedoya, issued a statement urging legislators who want to see greater protections against biometric surveillance to write those protections into legislation and emphasized the need for companies to obtain explicit consent before deploying such technology due to its potential impact on individuals' privacy rights.

Attorneys helping implement facial recognition systems should consider the following lessons from the FTC's settlement with Rite Aid:

- **Conduct Rigorous Product Safety; Screen for Biased Results.** Any systems that make predictions about individuals risk producing biased results. The FTC has shown an interest in policing such potential bias, so any company developing technology should document screening against gender and ethnic bias. Such bias assessment should be part of a broader product safety/privacy review process that documents any risks to consumers and how the company mitigates such risks (such assessments should include but go beyond privacy impacts arising from personal data processing). Rite Aid will be required to conduct such assessments annually, so make your risk assessments living documents that are refreshed at repeating intervals.
- **Images and Voice Recording should be Viewed Similarly to Traditional Biometrics.** Biometrics refers to bodily measurements capable of directly identifying a specific individual under older legal regimes (e.g., under BIPA and security incident response laws). The FTC broadly defines the concept to include data that isn't directly identifying, such as images or sound recordings, in the Rite Aid settlement.
- **Don't Retain Identifiable Data Indefinitely.** Based on this ruling and prior FTC guidance, companies should establish and enforce retention and data governance schedules listing how long the company retains biometrics and for what purposes.
- **Provide Notice of Entry into Databases; Access Right in Conflict.** Rite Aid must notify a consumer before entering the consumer's face into smart security databases (unless there are safety reasons for avoiding such notice) and mandates certain disclosures in online privacy notices. The FTC's settlement also creates rights for consumers to access samples of their biometric information. Such rules are curious for a couple of reasons. First, those requirements give individuals privacy rights in information used to cooperate with law enforcement and protect Rite Aid's safety and security (which are sometimes excluded from consumer privacy rules). Second, other privacy regimes, such as the CCPA, would prohibit providing such access rights given the risk of providing highly sensitive data (i.e., the biometrics) to a fraudulent requestor.
- **Training - Make Personnel Aware of Controls.** The FTC has emphasized in multiple enforcement actions that organizations using biometrics (especially for A.L. and machine learning development) should train applicable personnel on how the organization secures the limits the use of biometrics.