Updates

The Federal Trade Commission (FTC) announced its first enforcement action alleging that discriminatory use of artificial intelligence (AI) was an unfair practice under Section 5 of the FTC Act on December 19, 2023.

According to the FTC's complaint against Rite Aid, when the retail pharmacy chain implemented facial recognition technology in a subset of its stores as an anti-shoplifting and security tool, it failed to implement reasonable safeguards to prevent false positives, i.e., instances where the technology misidentified customers as individuals who had previously engaged in shoplifting or other problematic behavior, including by failing to take steps to assess or address the disproportionate risks of misidentification based on a customer's race or gender. The FTC also alleges that Rite Aid failed to use reasonable steps to select and retain service providers capable of appropriately safeguarding consumers' personal information they received from Rite Aid, in violation of a 2010 FTC consent order. The FTC's proposed consent order bans Rite Aid, which is presently in bankruptcy

proceedings, from using facial recognition or analysis systems in any physical retail store or pharmacy, or any online retail platform, for five years, and if Rite Aid deploys an automated biometric security or surveillance system, it must establish, implement, and maintain a comprehensive mandatory program to identify, assess, and monitor the risks associated with that technology.

The enforcement action signals that, following a number of earlier warnings about algorithmic fairness and the potential for misuse of biometrics systems, including a policy statement on biometric information, the FTC is using and will continue to use its Section 5 unfairness authority to require reasonable safeguards on the use of automated tools, including those relying on facial recognition and other biometric technology, to ensure their accuracy and absence of bias. What is more, the case provides the most concrete guidance from the FTC to date regarding the measures that the FTC would like to see companies take to help ensure that AI systems operate accurately and without bias.

The FTC's Allegations Against Rite Aid

According to the complaint, Rite Aid used facial recognition technology in its efforts to identify "persons of interest," i.e., individuals it had previously flagged as engaged in shoplifting or other behaviors deemed problematic. When Rite Aid believed an individual had engaged in criminal activity, Rite Aid "enrolled" in its "watchlist" database an image of that individual, with identifying information, if available. Rite Aid then used facial recognition technology to compare customers' faces from security camera footage against the enrolled images in its watchlist database, and employees received alerts about potential "matches." Based on these alerts, which the complaint alleges were often false positives, employees took action against numerous individuals, such as surveilling and following customers around Rite Aid stores, instructing customers to leave and preventing them from making needed purchases, and wrongly accusing individuals of shoplifting in public in front of coworkers, family, and friends.

Unfair Facial Recognition Technology Practices

The FTC alleges that Rite Aid used facial recognition technology unfairly by failing to adequately address the risks of using the technology without taking steps to mitigate the harm to consumers arising from being misidentified as a "person of interest," such as restricting their ability to make purchases, severe emotional distress, reputational harm, or wrongful arrest. More specifically, the complaint alleges a host of failures to take reasonable steps to reduce the risks of false positives, such as:

- **Failure to pre-test for accuracy.** Not seeking any information from its facial recognition technology vendors about the extent to which their facial recognition technology had been tested for accuracy and not obtaining, reviewing, or relying on the results of any such testing before implementing the technology, even though the vendors expressly disclaimed the accuracy of their technology.
- **Failure to enforce image quality controls.** Allowing the system to enroll images that did not meet the quality standards Rite Aid itself had set and which increased the risk of false positives such as because the images were blurry or were taken in poor lighting.
- **Failure to monitor, assess, or test accuracy of results.** Failing to monitor, assess, or test the accuracy of the results after the technology was deployed, such as by not testing match alert accuracy (e.g., by instructing employees to ask for a patron's identification before asking them to leave a store) and not fixing problematic "watchlist" enrollments, including examples where a single enrollment led to hundreds of "match alerts," many of which were on the other side of the country from the location of the enrollment.
- **Failure to train and oversee employees.** Failing to adequately train or oversee employees using the technology. Although it was Rite Aid's policy that employees authorized to operate facial recognition technology should receive approximately one to two hours of training on its facial recognition system, in nearly all cases, Rite Aid allegedly did not verify or obtain any record that employees had received such

training.

In addition, the FTC alleges that Rite Aid failed to assess or address risks that the facial recognition technology would disproportionately harm consumers because of their race or gender, including by:

- **Disproportionate deployment in urban areas.** Unevenly deploying the technology in "urban" areas and other locations where it would disproportionately affect certain populations, such that store patrons "in plurality-Black, plurality-Asian, and plurality-Latino areas were more likely to be subjected to and surveilled by Rite Aid's facial recognition technology."
- **No effort to assess technology post-deployment.** Making no effort before or after implementing the technology to assess, test, inquire, or monitor whether it was "especially likely to generate false positives" depending on a person's race or gender, despite the technology having lower confidence scores in stores located where the plurality of patrons were Black or Asian or on enrollments with typically feminine *names*.

Unfair Data Security Practices

Separate from its allegations of discriminatory AI practices, the FTC also asserted that Rite Aid did not take reasonable steps to oversee service providers who received personal information from Rite Aid, in violation of a 2010 consent order, which required that Rite Aid institute a comprehensive information security program. The complaint alleges that Rite Aid failed to comply with the prior order and its own written information security policies by, for example:

- Not documenting information about potential service providers' ability to appropriately safeguard personal information.
- Not maintaining risk assessment documentation for vendors, failing to consistently reassess vendors' information security programs, and ignoring risk assessments it *did* receive.
- Contracting with service providers who lacked or only had minimal information security requirements.
- Failing to include language regarding Rite Aid's breach notification requirements in contracts it executed with service providers.

Requirements in the Consent Order

The FTC's consent order, which is set to last for 20 years (as is typical for FTC consent order settlements), bars Rite Aid from using or assisting in the use of facial recognition or analysis systems in any retail store or pharmacy or any online retail platform for five years. It also mandates the following key measures:

- **Algorithmic disgorgement and data deletion.** The order requires Rite Aid to destroy all photos and videos collected in connection with a facial recognition system, as well as any data, models, or algorithms derived from them, and to instruct any nongovernmental third parties that received any such photos, videos, data, models, or algorithms to delete those materials and provide written confirmation of such deletion.
- **Mandatory automated biometric security or surveillance system monitoring program.** If Rite Aid chooses to use any automated biometric security or surveillance systems in any retail store, pharmacy, or online retail platform (including a facial recognition system after the five-year ban), it must establish, implement, and maintain a comprehensive monitoring program in order to (1) identify and address any risks that the system will result in physical, financial, or reputational harm to consumers, stigma, or severe emotional distress; and (2) identify and address risks that any such harms will disproportionately address consumers based on race, ethnicity, gender, sex, age, or disability. This program requirement is in concept broadly modeled on the FTC's mandatory information security programs in that it is a process-based

requirement (while specifying certain mandated safeguards), and its key features include the following requirements:
    - **Oversight.** Designate a qualified employee or employees to coordinate and be responsible for the program, which must be documented in writing.
    - **Risk assessment.** Conduct written predeployment assessment that evaluates, at a minimum, the risks that consumers could experience, such as physical, financial, or reputational injury, stigma, or severe emotional distress, in connection with any inaccurate outputs from the system (e.g., if the technology misidentifies a consumer).
    - **Safeguards to address identified risks.** Implement measures to address the identified risks, including selecting service providers with sufficient information security practices, regular and annual training for any employee who uses the system, and documenting (1) inaccurate system outputs, (2) steps taken due to inaccurate outputs, and (3) steps taken to remedy actions based on inaccurate outputs.
    - **Periodic reevaluation.** Before deploying an AI-based biometric security system, and every 12 months afterward, evaluate and adjust the system in light of any circumstance that may materially affect its effectiveness. Afterward, Rite Aid must timely implement modifications to address any identified risks that consumers may experience physical, financial, or reputational injury, stigma, or severe emotional distress.
    - **Monitoring.** Document and monitor the automated biometric security or surveillance system's accuracy.
- **Notice and complaint procedures.** Rite Aid must provide written notice to all consumers who are enrolled in any database the system matches against, as well as to all consumers against whom Rite Aid takes action based on the output of the system (with limited exceptions for safety concerns or the nature of a security incident). The notices must include, among other things, contact information to submit complaints, and Rite Aid must investigate each complaint and provide a confirmation of receipt within seven days and a substantive written response within 30 days.
- **Retention limits for biometric information.** Rite Aid must develop and implement a retention schedule for biometric information and may not retain any biometric information it collects for longer than five years.
- **Clear disclosure of use of biometric security or surveillance systems.** Rite Aid must post notices about its collection of biometric data and use of any automated security system in *each* location it collects or uses such data.
- **Mandatory information security program with outside assessments and covered incident reports.** The order includes the FTC's standard requirement of a comprehensive information security program with assessments by a third party (with certain mandated safeguards specified), as well as the requirement that has become more common in recent orders, of reporting of certain data security incidents to the FTC.

Takeaways

The settlement gives teeth to the FTC's earlier statements about algorithmic fairness and misusing biometric technologies. Some key takeaways from the substantial complaint and consent order include the following:

- **Nationwide regulation of biometric technology.** Biometrics issues now clearly present an issue of federal law under Section 5 of the FTC Act, as well as an issue under state and local biometric-specific statutes or regulations. The FTC is applying Section 5 to regulate not only issues regarding whether biometric information was collected and used with appropriate notice and consent (as in the *Everalbum* settlement of a deception claim regarding such issues), but also substantive concerns over the impact of inaccuracies and bias in the algorithms themselves through its unfairness authority.

- **Users of technology, not just developers, are responsible for its accuracy and absence of bias.** Notably, Rite Aid retained vendors who provided the facial recognition technology at issue in this case; it did not develop that technology itself. Nonetheless, the FTC held Rite Aid responsible for testing and vetting the accuracy of that technology as Rite Aid would use it before and during its deployment. Companies that retain vendors to provide AI technology should give careful consideration to how to test that technology before deploying it in a consumer context.
- **Rigorous new "baseline" regime for biometric compliance programs.** The process-based mandated automated biometric security or surveillance system monitoring program sets out the most detailed guidance to date regarding the steps the FTC would like companies to take before relying on automated systems to make decisions that are likely to result in substantial injury to consumers. Notably, while the requirements the order lays out are extensive, Commissioner Alvaro M. Bedoya describes the mandated program as only a "*baseline* for what a comprehensive algorithmic fairness program should look like." And notwithstanding that this order did not appoint an independent assessor to conduct biannual compliance reviews (as is typical in orders that mandate a comprehensive security or privacy program), Commissioner Bedoya warns companies to expect such provisions in future orders.
- **Algorithmic disgorgement remedy becoming standard.** In a spate of recent cases such as *Everalbum*, the FTC has required companies to "disgorge" not only the data it alleges was collected unlawfully, but also any data, models, or algorithms derived therefrom. Companies should generally expect this provision to be proposed in future FTC settlements as a remedy for allegations of misuse of data in connection with machine learning (ML), biometric, or other AI systems.

The *Rite Aid* case reflects that the FTC is paying close attention to the implementation of biometric and other AI technologies in consumer settings, particularly if they are perceived to cause disproportionate harm based on race or gender. And the consent order shows that the FTC expects a high degree of care and forethought by businesses prior to, and after, deployment of the technology.

Authors

Erin K. Earl

Partner
EEarl@perkinscoie.com 206.359.8510

Janis Kestenbaum

Partner
JKestenbaum@perkinscoie.com

Saroop Sandhu

Associate
SSandhu@perkinscoie.com 650.838.4328

Explore more in

Privacy & Security Technology Transactions & Privacy Law Artificial Intelligence & Machine Learning

Related insights

Update

Employers and Immigration Under Trump: What You Need To Know

Update

‘Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers