Skadden

AInsights

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Michael W. McTigue Jr.
Partner / New York
212.735.3529
michael.mctigue@skadden.com

Meredith C. Slawe
Partner / New York
212.735.3534
meredith.slawe@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

Proposed FTC Order Suggests Blueprint for AI Adoption

A proposed settlement action filed on December 19, 2023, by the Federal Trade Commission (FTC) against Rite Aid Corp. highlights some of the key issues presented when companies use artificial intelligence (AI) for facial recognition surveillance, and provides a blueprint for how companies can minimize their risk of deploying such systems. The settlement was filed as a complaint and proposed stipulated order by the FTC in the U.S. District Court for the Eastern District of Pennsylvania, and must be approved by that court as well as the court overseeing Rite Aid's bankruptcy.[1]

FTC's Allegations Against Rite Aid

The FTC alleged that between October 2012-July 2020, unbeknownst to customers, Rite Aid used an AI-enabled third facial recognition tool at certain of its retail pharmacy locations to identify customers that it had previously deemed likely to engage in shop-lifting or other criminal behavior. In stores where this technology was deployed, cameras captured images of consumers who entered the store and matched them against Rite Aid's "watchlist database." Rite Aid had built that database with its own low-quality images of individuals who had engaged in actual or attempted criminal activity at a Rite Aid store and with "Be On the Look Out" information it had obtained from law enforcement. Where available, the database also included other information about the individual, such as their first and last names, birth year, and information about the behavior in which they had allegedly engaged.

When the technology found a match, store employees were alerted along with one of a series of directions, including whether to approach the consumer and ask them to leave or notify law enforcement. While the technology generated a score about the "confidence" of the match, employees were not given this score. According to the FTC, the technology generated thousands of "false positives," particularly among Black, Asian, Latino and women customers. This included cases where an individual was inaccurately "matched" in numerous California and New York stores within a 24-hour period.

The crux of the FTC's complaint was that Rite Aid failed to take appropriate steps when deploying this technology, including:

- Failing to consider or address the foreseeable harm to consumers, including risks associated with a higher rate of false positives based on race or gender. The FTC alleged that Rite Aid was aware of this risk based on patterns in the confidence scores being generated by the technology, but failed to act on it.

[1] Unrelated to this matter, Rite Aid Corporation and Rite Aid Hdqtrs. Corp. filed petitions for relief under Chapter 11 of the Bankruptcy Code on October 15, 2023.

- Failing to adequately test the system's accuracy before deploying it or asking the vendors it used about the extent of their own testing. The FTC also noted that the vendors Rite Aid used had disclaimed the accuracy of their technology in their contracts with Rite Aid.
- Failing to use high-quality images so the technology functioned properly, even though Rite Aid knew such images were necessary.
- Failing to take reasonable steps to train and oversee its employees who used the technology, or informing them of the risks to consumers from using the technology.
- Failing to take reasonable steps to monitor the technology, including (i) verifying or testing the accuracy of match alerts, (ii) tracking the rate of false-positive matches and (iii) remedying problems with images in its database after false-positive issues had been identified.

The FTC alleged that these false-positive matches caused or were likely to cause substantial consumer injury, including by mistakenly identifying customers as shoplifters and causing them emotional distress, preventing them from purchasing products they may need — including medications — and subjecting them to unwarranted searches. Based on the foregoing, the FTC claimed that Rite Aid had violated Section 5 of the FTC Act.[2]

The FTC Order

The FTC Order (the Order) imposes the following requirements on Rite Aid:

- Rite Aid is prohibited from deploying any "Facial Recognition or Analysis System" in any retail store or pharmacy or on any online retail platform. A Facial Recognition or Analysis System is generally defined as a system or algorithm that uses "depictions or images, descriptions, recordings, copies, measurements, or geometry of or related to an individual's face" to generate an output used for security or surveillance purposes.
- Within 45 days of the Order, Rite Aid must delete or destroy all photos and videos of consumers used or collected in connection with the operation of its Facial Recognition or Analysis System prior to the effective date of the Order, as well as "any data, models, or algorithms derived in whole or in part therefrom."
- Within 60 days of the Order, Rite Aid must notify all third parties that received such materials about the scope of the Order, and require them to delete or destroy these materials.
- To the extent that, going forward, Rite Aid uses any system that uses any biometrics for security or surveillance (System) that is not otherwise prohibited under the Order, Rite Aid must implement a written "comprehensive Automated Biometric Security or Surveillance System Monitoring Program" (Program). This Program must, among other requirements:
  - Identify and address any risks to the "physical, financial, or reputational harm to consumers, stigma, or severe emotional distress, including in connection with communications of any [results] to law enforcement or other third parties."
  - Identify and address the risk of disproportionate harm based on race, ethnicity, gender, sex, age or disability.
  - Prior to deploying a System, and annually thereafter, conduct a security assessment (Security Assessment) that considers a variety of factors, including how these Systems were developed and the data on which they were trained, in which locations the Systems will be deployed and for how long, the likelihood of inaccurate results, factors that might increase the probability of inaccurate results, and the consequences of such inaccurate results.
  - Implement, maintain and document safeguards designed to control for the risks identified in the System Assessment, including keeping records of any inaccurate results, removing biometric information that has resulted in two or more inaccurate results, and annually testing the System.
- Rite Aid may not deploy a System unless it possesses "competent and reliable scientific evidence that is sufficient in quality and quantity based on standards generally accepted in the relevant scientific fields, when considered in light of the entire body of relevant and reliable scientific evidence," to substantiate that results are likely to be accurate.
- Rite Aid must provide consumers with notice that their biometric information has been included in the System unless it is unable to do so due to safety concerns or the nature of a security incident, and a means to lodge a complaint about the System. As part of such notice, Rite Aid must inform the consumer why their biometric information has been included (including a description of the incident that triggered inclusion), the type of information included and how long it will be retained for. Rite Aid must acknowledge it received a complaint within seven days of receipt and provide a response to the complaint within 30 days.
- Biometric information cannot be retained for more than five years unless Rite Aid has obtained affirmative express consent from the consumer to do so.

[2] The FTC also alleged in the same complaint that Rite Aid violated the terms of its 2010 FTC order requiring Rite Aid to maintain a comprehensive information security program. This claim was unrelated to the issues with the facial recognition technology.

Proposed FTC Order Suggests Blueprint for AI Adoption

- Rite Aid must provide clear and conspicuous notice at each retail location where a System is used — and on each online and mobile device where biometric information is collected — about the System, including what biometric information is collected, why the System is being used and what is done with the results.

Takeaways

The FTC's complaint and order highlights the bias risk attendant to certain AI systems used for facial recognition. While the alleged conduct took place between 2012-2020, and advances have been made in facial recognition technology since that time period to try and minimize such biases, these risks are still present. The FTC order therefore provides a useful blueprint for companies seeking to deploy facial recognition technology, and more generally any type of AI-based technology. The order also provides insights into how the FTC is looking at these issues. Indeed, FTC Commissioner Alvaro Bedoya said in a statement accompanying the Order that it provides "a baseline for what a comprehensive algorithmic fairness program should look like." These steps include:

- Implementing testing and security/risk assessments both prior to deploying a System and periodically thereafter to identify and mitigate any risks, including by considering generally accepted scientific standards.
- Training employees prior to the use of a System, and refreshing that training on a periodic basis.
- Creating a comprehensive written program regarding the deployment, use and maintenance of the System.
- Being mindful of how long biometric information is being stored.
- Considering the type of consumer notice that may be warranted.

Overall, the FTC, including through its Chairperson Lina Khan, has made clear that the agency will look closely at how companies are implementing AI and its impact on consumers. This matter highlights that the FTC is prepared to move against companies it believes have not taken adequate steps to protect consumers from injury, including requiring companies to delete the models built on data that was gathered or used improperly — so-called "algorithm disgorgement." Commissioner Bedoya also cautioned in her statement that companies that violate the law when using AI systems in the future "should be ready to accept the appointment of an independent assessor to ensure compliance."

More generally, companies that use biometric data and have been focused on compliance with applicable state laws — such as the Illinois Biometric Information Privacy Act — should take note that the FTC has also taken a strong interest in the use, collection and storage of such data, and is likely to be active in this space as well.