AI Faces New Challenges as FTC Agrees to Novel Settlement with Rite Aid Over Use of AI and Biometric Information

Daniel GoldbergZach Lewis, December 29, 2023

On December 19, 2023, the FTC announced that it has entered into a tentative settlement with Rite Aid after bringing charges of "unfair facial recognition technology practices" over Rite Aid's use of AI / biometric information (see the complaint and proposed order).

While the press release highlights the ban on Rite Aid from using facial recognition technology f five (5) years, the proposed order goes far beyond regulating facial recognition technology or personal information, and may prove to be the FTC's biggest AI decision to date. Companies tha use AI technologies, especially those with brick-and-mortar stores, should carefully review the press release and documentations.

To see why, continue reading or skip directly to our **Takeaways** section below.

Rite Aid's Facial Recognition Technology Practices

The FTC's complaint is divided into two sets of allegations: first, that Rite Aid unfairly used facial recognition technology in its stores in violation of Section 5 of the FTC Act, and second, that Rite Aid's practices around its use of such technology violated its 2010 consent order with the FTC which required Rite Aid to "implement and maintain a comprehensive information security program." For purposes of this blog, we primarily focus on the first set of allegations.

According to the FTC's complaint, from 2012 to around 2020, Rite Aid utilized facial recognition technology within its stores to identify potentially problematic customers so that Rite Aid could remove them to reduce theft and related issues. Rite Aid worked with two vendors to deploy this facial recognition technology, which operated as follows:

1. Rite Aid created an internal database of individuals it deemed "persons of interest." Each entry in the database had an "enrollment image" of the individual, which Rite Aid obtained from security cameras, law enforcement agencies, media reports, and other

sources, along with accompanying information such as the individual's name, birth year, and criminal behavior.
2. Rite Aid captured live video footage from its in-store closed-circuit television (CCTV) cameras, and fed the video through the vendors' facial recognition technology system;
3. The facial recognition technology scanned faces within the video feed and, using AI, compared those faces to the enrollment images maintained by Rite Aid;
4. When the facial recognition technology identified a match between a face in the video feed and a face in the database, the vendors would send a notice to employees' cell phones that "person of interest" entered the store. The technology generated a confidence score along with the images, but the "match alert" sent to Rite Aid employees generally did not include those scores.
5. The match alert would instruct Rite Aid employees on how to respond, and the employee would take action based on the instructions, which ranged from asking the customer to leave to calling 911 and telling police that "a potentially violent or dangerous subject has entered the store."

Further according to the complaint, Rite Aid instructed its employees to "push for as many enrollments as possible" and "not to reveal" the use of the technology to consumers or the media. Over the years, Rite Aid enrolled tens of thousands of people in its database, which were retained indefinitely.

Allegations

The FTC alleged that Rite Aid's facial recognition technology practices were problematic. Specifically, Rite Aid allegedly:

- failed to provide any notice to consumers of its use of the facial recognition technology
- failed to test or discover the accuracy of the facial recognition technology before deployment;
- failed to consider the risks to consumers, including, for example, that false positive matches could lead to a restriction of a consumer's ability to make needed purchases, severe emotional distress, reputational harm, or even wrongful arrest;
- failed to consider disproportionate harm to consumers because of their race, gender, or other characteristics;
- failed to enforce image quality standards necessary for the system to function as intended, and instead used enrollment images that were low quality;
- failed to train and oversee employees charged with operating the technology, including educating them about the likelihood of false positive matches;
- failed to regularly monitor and assess the accuracy of the facial recognition technology including by recording outcomes or tracking false positive matches;

- failed to remedy problematic enrollment images, even when the same image was generating numerous false positive matches; and
- failed to implement reasonable security around the facial recognition technology, including vetting, periodically reassessing, and imposing security obligations on the vendors.

As a result, the technology allegedly produced thousands of false positive matches (match alerts that incorrectly flagged someone as an individual in the database). For example, in the span of five (5) days, the technology generated over 900 match alerts for one specific individual in over 130 locations, a majority of the stores where the technology was used.

The FTC claimed Rite Aid employees wrongly took action against customers triggering false positive matches including "subjecting them to increased surveillance; banning them from entering or making purchases at the Rite Aid stores; publicly and audibly accusing them of past criminal activity in front of friends, family, acquaintances, and strangers; detaining them or subjecting them to searches; and calling the police to report that they had engaged in criminal activity." According to the FTC, these "unfair practices" resulted in physical, financial, emotional and reputational harm to consumers and had a disparate impact on women and people of color.

Proposed Order

In settling the FTC's charges, Rite Aid agreed to a proposed order that is incredibly comprehensive. Under the proposed order, which is effective for twenty (20) years:

- Rite Aid is prohibited for five (5) years from deploying any "Facial Recognition or Analysis System" (FRAS) (more on that defined term below) in any retail store, retail pharmacy, on online retail platform.
- Within 45 days, Rite Aid must destroy all photos and videos of consumers collected in connection with the operation of any FRAS, as well as any data, models, or algorithms derived therefrom, and provide a written statement to the FTC confirming its compliance.
- Within 60 days, Rite Aid must identify all third parties that received photos and videos of consumers used or collected in connection with the operation of any FRAS and any data models, or algorithms derived therefrom, and instruct such third parties to destroy them.
- Rite Aid is prohibited from making misrepresentations around privacy and security measures.
- Within 90 days, Rite Aid must establish a comprehensive information security program It must also obtain initial and biennial assessments of the information security progra and notify the FTC of any security incidents affecting 500 or more consumers.

- Rite Aid's CEO must provide annual certifications to the FTC documenting compliance with the order.
- Rite Aid is prohibited from using any "Automated Biometric Security or Surveillance System" (ABS) (a term that includes FRAS, more on that below) in connection with Biometric Information (again discussed below) collected from consumers in connectio with operation of any retail store, retail pharmacy, or online platform, UNLESS:

1. The system does not qualify as a FRAS

2. Rite Aid first establishes and maintains a comprehensive program for the ABS with specific requirements set out in the proposed order, including that Rite Aid:
    - address risks that operation of the ABS will result, in whole or in part, in physical, financial, or reputational harm to consumers, stigma, or severe emotional distress including in connection with communications to law enforcement or other third parties;
    - identify and address risks that any such harms will disproportionately affect consumers based on race, ethnicity, gender, sex, age, or disability, alone or in combination;
    - within ninety (90) days of the order, and thereafter at least once every twelve (12) months, conduct a written assessment of potential risks to consumers from the use of the ABS;
    - Implement, maintain, and document safeguards that are designed to control for the risks identified in that assessment based on the severity of the risk to consumers and the likelihood that the risk could be realized
    - Evaluate and adjust the program in light of any circumstance Rite Aid has reason t know may materially affect the program's effectiveness;
    - At a minimum, every twelve (12) months, evaluate the effectiveness of the prograr in light of the assessment and the results of all related monitoring, testing, and documentation;
    - Provide the written assessment and program, and any evaluations thereof or updates thereto, to its board of directors
    - Designate a qualified employee or employees to coordinate and be responsible fc the program
    - Not deploy (and discontinue deploying) any ABS if Rite Aid does not have competent and reliable scientific evidence to substantiate that its outputs ar likely to be accurate, or if it has reason to believe the ABS creates a risk that inaccurate outputs will cause substantial physical, financial, or reputational injury, discrimination based on race, ethnicity, gender, sex, age, or disability, stigma, or severe emotional distress to consumers

3. Rite Aid first establishes and maintains procedures to provide consumers with notice and a means of submitting complaints relating to outputs of the ABS, and more specifically:
    - Provide written notice to all consumers who will have their Biometric Information enrolled in any collection or database used in conjunction with an ABS, including an explanation for the reasonable basis for enrollment, instructions about how to obtain a copy of the sample of Biometric Information that was collected (which Rit Aid must make available upon request as long as it is retained), the length of time for which Rite Aid will retain the consumer's Biometric Information, and contact information for consumers to submit complaints or inquiries
    - Provide notice to all consumers against whom Rite Aid takes an action that can result in physical, financial, or reputational harm (unless it is unable to provide such notice due to safety concerns or a security incident), with such notice to include: the date, approximate time, and location of the ABS output; a description of the actions taken; an explanation as to how that relates to the output; and contact information for consumers to submit complaints or inquiries
    - Investigate each complaint to determine whether the relevant output was inaccurate (and identify any factors that likely contributed to the generation of an inaccurate output) and assess whether the response to the output was appropriate; and
    - Respond to each consumer complaint relating to the ABS twice: first within seven (7) days of receipt, providing written confirmation of receipt, and again within thirt (30) days of receipt, providing a written response stating whether the output was determined to be inaccurate, the basis for that determination, and the actions taken in response to the complaint

4. Rite Aid first develops and implements, for each type of Biometric Information collected, a written retention schedule setting forth:
    - All purposes and business needs for which it collects or uses the of Biometric Information;
    - A timeframe for deletion of the Biometric Information that is no greater than five (5) years, except to the extent that retention beyond five years is required by law c Rite Aid obtained affirmative express consent for the retention within the previous five (5) years; and
    - The basis for the timeframe for deletion of the Biometric Information, including any foreseeable effect of the passage of time since the Biometric Information was collected on the likelihood of inaccurate outputs

5. Rite Aid posts clear and conspicuous notices in each physical retail location and on each online service where Biometric Information is collected. The notice must contain specific disclosures, including

- The specific types of Biometric Information that are collected for the purpose of operating an ABS
- The types of outputs that are generated by the ABS
- All purposes for which Rite Aid uses each ABS or its outputs, including actions that may be taken based on outputs
- The timeframe for deletion of each type of Biometric Information uses

This is not an exhaustive list of definitions or Rite Aid's obligations.

The proposed order also includes the following key definitions:

- "*Facial Recognition or Analysis System*" (FRAS) means an ABS that "analyzes or uses depictions or images, descriptions, recordings, copies, measurements, or geometry of or related to an individual's face to generate an Output."
- "*Automated Biometric Security or Surveillance System*" (ABS) means "any machine-based system, including any computer software, application, or algorithm, that analyzes or uses Biometric Information of, from, or about individual consumers to generate an Output that relates to those consumers, notwithstanding any assistance b a human being in such analysis or use, and that is used in whole or in part for a Security or Surveillance Purpose."
- "*Biometric Information*" means "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 depictions or images, descriptions, recordings, or copies of an individual's facial or other physical features (e.g., iris/retina scans), finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern))."
- "*Output*" means "a match, alert, prediction, analysis, assessment, determination, recommendation, identification, calculation, candidate list, or inference that is generated by a machine-based system processing Biometric Information."
- "*Security or Surveillance Purpose*" means "a purpose related to surveillance (including but not limited to tracking individuals' location or behavior without Affirmative Express Consent); the detection, deterrence, prediction, or investigation of theft, crime, fraud, or other misconduct; or access to locations, material goods, information, systems, or networks."

Takeaways

The FTC is cementing its role as a key regulator of AI technology. The proposed order may ultimately be remembered as the first AI decision, not a privacy decision. Regulating data flows i only one area of concern for the FTC; the order makes clear that the FTC is very much focused

on the underlying technology and the impact of the technology on consumers, as further discussed below.

The FTC is looking to regulate more than facial recognition technology. At 28 pages long, the FTC order is robust. While the 5-year prohibition on Rite Aid deploying facial recognition technology is making headlines, the real substance of this order comes from the inclusion of requirements around Rite Aid's use of any Automated Biometric Security or Surveillance System (ABS). Facial recognition technology is just one type of ABS, and the FTC has included extensiv requirements that apply to Rite Aid's use of any ABS, not just facial recognition technology.

The FTC is concerned about algorithmic fairness and bias. Much of the proposed order relates to preventing algorithms that generate inaccurate outputs that cause substantial harm to consumers or discriminate based on race, gender, or similar basis. Expect the FTC to bring further actions based on these concerns.

The proposed order provides guidance on the FTC's expectations for AI assessments. As noted above, prior to deploying any ABS, Rite Aid must, among other things, establish and maintain a comprehensive internal assessment program that requires the evaluation of algorithmic outputs, in particular for algorithmic fairness and bias. The FTC dedicates 7 pages o the order describing this program, meaning it is incredibly important to the FTC. Notably, these assessment requirements go beyond regulating privacy - they regulate the use of AI technology.

The FTC's broad terminology arguably captures unintended services. As you can see from the definitions above, ABS is so broadly defined that it arguably includes any technology that runs analysis on human bodies, even if that technology doesn't have similar concerns around algorithmic fairness or bias. While facial recognition technology clearly falls within scope of an ABS, other examples may be less evident. Imagine you own a retail store and want to know the number of consumers who visit your store on a daily basis and the path consumers walk within your store in order to determine product placement. Many vendors now offer AI solutions that identify colors and patterns within video feed and plot consumer vector paths over various images without requiring facial data. These technologies arguably involve the use of “gait” or other bodily features, which the FTC defines as Biometric Information. Unlike most state privacy laws, the FTC's definition of Biometric Information does not include an “intent to identify” standard. In other words, using one of these vendor AI solutions, even where a retail company only wants aggregate data about consumer movement, could still trigger the definition and all th accompanying obligations.

Compliance with the proposed order will be nearly impossible. It is unclear how Rite Aid ca realistically comply with all the various requirements in this order, especially requirements aroun ABS use and the requirement to delete data models or algorithms and ensure third parties do th same. While this order is not the first time we have seen the FTC include the algorithmic disgorgement requirement, we do not yet know what the FTC expects for compliance.

Vendors take on huge risk. Rite Aid used vendor-provided facial recognition technologies for nearly a decade, so requiring Rite Aid's vendors to delete their data models or algorithms could effectively put them out of business if they used the data they obtained to improve their algorithms. The proposed order puts significant burden on downstream vendors to ensure the companies that use their products comply with the law.

Compliance with the proposed order may conflict with other laws. One particularly expansive aspect of the order is that the requirements apply to both in store and online platform This could be problematic if Rite Aid wanted to roll out an online technology to comply with othe state laws (often aimed at protecting children), such as an online age verification tool using facia features for purchasing alcohol online, or similar services.

The costs of compliance may outweigh the benefits of using an ABS. Even if Rite Aid coul comply, the order requires such a detailed analysis of the potential harms to individuals arising from any ABS that the costs and risk of non-compliance likely outweigh the expected benefits of using that technology.

Rite Aid's bankruptcy and prior consent order may have played a role in the settlement. This order likely came out more extreme than usual due to the unique circumstances. First, Rite Aid is involved in bankruptcy proceedings, and may have agreed to take on robust compliance obligations in exchange for not incurring costs of litigation and avoiding significant fines that could adversely impact its bankruptcy proceedings or creditors. Second, the FTC alleged Rite Aid violated its prior consent order, which gave FTC grounds for a more robust penalty.

The order may be akin to "poison pill" for Rite Aid. Although Rite Aid was able to avoid a monetary penalty, the prohibitions and burdensome requirements in the order may ultimately deter investors, competitors, or other would-be acquirers from taking control of Rite Aid, or decrease the value of its assets.

Having appropriate information and data security programs and disclosures, as well as ongoing AI ethics and technology training, is crucial to mitigate potential risks arising

from AI, ABS, and similar technologies.

Final Thoughts

Along with the proposed order, FTC Commissioner Alvaro Bedoya released a statement containing an excerpt that sums up the FTC's stringent position on AI technology: "no one shoul walk away from this settlement thinking that [the FTC] affirmatively supports the use of biometric surveillance in commercial settings . . . there is a powerful policy argument that there are some decisions that should not be automated at all; many technologies should never be deployed in the first place." Companies in every industry should carefully evaluate their use of AI technology and prioritize proper governance and consumer protection.