AN A.S. PRATT PUBLICATION
MARCH-APRIL 2024
VOL. 10 NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 3** **March-April 2024**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

More Than a Ban on Facial Recognition Use: The Federal Trade Commission's Rite-Aid Action and Proposed Stipulated Order

By Matthew D. Provance and Britteny L. Leyva*

In this article, the authors examine a recent enforcement action brought by the Federal Trade Commission that offers insight into the potential consequences for businesses that do not comply with the agency's policy statement guidelines.

The Federal Trade Commission (FTC) warned businesses of its stance on the use and collection of biometric information in a May 2023 policy statement.[1] Now, a recent enforcement action[2] offers insight into the potential consequences for businesses that do not comply with the FTC's policy statement guidelines.

The FTC has sued[3] Rite-Aid Corporation and its parent company Rite-Aid Headquarters Corporation (together, Rite-Aid) in the U.S. District Court for the Eastern District of Pennsylvania for (1) an unfair Facial Recognition Technology (FRT) practice, improperly using FRT that falsely flagged Rite-Aid customers for shoplifting, and (2) failing to implement a comprehensive security program to protect customers' personal information. The complaint alleges that Rite-Aid's failure to take reasonable measures that would prevent harm to consumers violated a 2010 consent order[4] (2010 order) with the FTC and Section 5 of the FTC Act.[5]

The FTC attached a stipulated order to its complaint that, if approved, would not only ban Rite-Aid from using FRT for five years but also require significant modification to Rite-Aid's existing information security policies.

BACKGROUND

The FTC filed an administrative complaint[6] on November 12, 2010, against Rite-Aid for failing to implement reasonable and appropriate security measures to prevent unauthorized access to personal information. Rite-Aid later agreed to the 2010 order, which required it to (1) implement and maintain a comprehensive information security program, and (2) retain documents relating to its compliance with that provision of the order.

---

* The authors, attorneys with Mayer Brown, may be contacted at mprovance@mayerbrown.com and bleyva@mayerbrown.com, respectively.

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf.

[2] https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.

[3] https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_complaint_filed.pdf.

[4] https://www.ftc.gov/sites/default/files/documents/cases/2010/07/100727riteaidagree.pdf.

[5] 15 U.S.C. §§ 45(a), (n).

[6] https://www.ftc.gov/sites/default/files/documents/cases/2010/11/101122riteaidcmpt.pdf.

About 10 years later, in 2020, Reuters published[7] an investigative report about Rite-Aid's use of FRT in its stores. As reported in Rite-Aid's SEC filings,[8] the FTC opened an investigation that same year into Rite-Aid's compliance with the 2010 order and followed up in 2022 with information requests related to Rite-Aid's procedure for ensuring that contracted vendors appropriately safeguard Rite-Aid costumer information.

In its new lawsuit, the FTC brings two claims against Rite-Aid under Section 5 of the FTC Act:

(1) Unfair FRT practices, and

(2) Failure to implement or maintain a comprehensive information security program as required by the 2010 order.

THE COMPLAINT

Unfair FRT Practices

The FTC alleges that between 2012 and 2020, Rite-Aid deployed artificial intelligence-based FRT to identify customers who potentially were shoplifting in its stores. According to the complaint, Rite-Aid maintained an enrollment database of images (along with other personal information) of people who it considered "persons of interest" because they had allegedly engaged in actual or attempted criminal activity at a Rite-Aid store or because Rite-Aid had received "Be On the Look Out" information about the individual from law enforcement. The FRT captured live images of individual shoppers in Rite-Aid stores and purported to match them with images from the enrollment database. If there was a match, the FRT would generate and send employees "match alerts" with instructions for handling the suspected shoplifter. The complaint faults Rite-Aid for allegedly failing to:

- Assess, consider, or take reasonable steps to mitigate risks to consumers associated with its implementation of FRT, including risks associated with misidentification of consumers at higher rates depending on their race or gender;
- Take reasonable steps to prevent its FRT from using low-quality images, increasing the likelihood of false-positive match alerts;
- Take reasonable steps to train or oversee employees tasked with operating FRT and interpreting and acting on match alerts; and
- Take reasonable steps, after deploying FRT, to regularly monitor or test the accuracy of the technology, including by failing to implement any

[7] https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

[8] https://www.sec.gov/Archives/edgar/data/84129/000155837023016503/rad-20230902x10q.htm.

procedure for tracking the rate of false positive facial recognition matches or actions taken on the basis of false positive facial recognition matches.

The FTC concluded that Rite-Aid's alleged conduct caused harm to consumers by:

(i.) Surveilling and following store customers around Rite-Aid stores;

(ii.) Preventing store customers from making needed or desired purchases (in the event employees were instructed to remove the consumer from the store);

(iii.) Subjecting consumers to unwarranted searches and calling the police on consumers who were falsely flagged as shoplifters, and

(iv.) Wrongly accusing store customers of shoplifting.

Unsurprisingly, the FTC's conclusions regarding Rite-Aid's alleged FRT practices appear to be based on the unfairness factors set forth in its May 2023 policy statement.[9]

FAILURE TO IMPLEMENT OR MAINTAIN A COMPREHENSIVE INFORMATION SECURITY PROGRAM

After addressing Rite-Aid's alleged improper use of FRT, the FTC then found Rite-Aid's existing information security program deficient because it failed to:

- Use reasonable steps for selecting and retaining capable service providers that appropriately safeguarded personal information;
- Require that service providers, by contract, implement and maintain appropriate safeguards for personal information; and
- Maintain written records relating to Rite-Aid's information security program.

The FTC concluded that Rite-Aid's conduct violated the 2010 order and that its violation is likely to cause substantial consumer injury.

THE STIPULATED ORDER

To settle the case, Rite-Aid agreed to comply with comprehensive information security policy mandates and ongoing reporting to the FTC. Rite-Aid is not required to pay a monetary fine. Among other things, the order[10] requires Rite-Aid to:

- Refrain from using FRT for five years;
- Delete biometric information collected by FRT;

---

[9] https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf.

[10] https://www.ftc.gov/system/files/ftc_gov/pdf/2023190_riteaid_stipulated_order_filed.pdf.

- Provide notice to third-parties of the FTC's complaint and order and require that these third-parties delete biometric information received from Rite-Aid;
- Provide the FTC with a list of all third-parties that received any of the following information from Rite-Aid:
    - A first and last name;
    - A home or physical address;
    - An email address or other online contact information, such as an instant messaging user identifier or a screen name;
    - A mobile or other telephone number;
    - A driver's license or other government-issued identification number;
    - A date of birth;
    - Geolocation information sufficient to identify street name and name of a city or town;
    - Bank account information or credit or debit card information (including a partial credit or debit card number with more than five digits);
    - A user identifier, or other persistent identifier that can be used to recognize a user over time and across different devices, websites, or online services;
    - User account credentials, such as a login name and password (whether plain text, encrypted, hashed, and/or salted);
    - Biometric information; or
    - Health information;
- Implement a comprehensive protocol for assessment, collection, maintenance, testing, retention, and safeguarding biometric information (if Rite-Aid intends to use a non-FRT biometric security system not subject to the five-year ban);
- Disclose the use of any non-FRT biometric security system to consumers in Rite-Aid stores via "clear and conspicuous" physical signs, and on each website, mobile app, or online service that collects biometric information;
- Disclose to consumers the specific types of biometric information collected, outputs generated by any non-FRT biometric security system,

purposes for collecting biometric information, and timeframe for deletion of each type of biometric information;

- Implement a comprehensive information security program;
- Retain a third-party assessor to periodically assess Rite-Aid's security program;
- Report data breaches of over 500 individuals to the FTC within 72 hours of Rite-Aid's reasonable belief of unauthorized access to covered information;
- Implement mandatory recordkeeping of Rite-Aid's revenue/sales; personnel records; consumer complaints; records related to compliance with the FTC's order; materials relied on for the mandatory system assessment; material different representations of Rite-Aid's privacy, security, availability, confidentiality, and integrity of any covered information; copies of the third-party assessor's report; subpoenas from law enforcement related to the FTC's order; and records showing lack of compliance with the FTC's orders; and
- Submit an annual certification of compliance with the FTC's order.

WHAT DOES THIS MEAN FOR BUSINESSES?

The Rite-Aid enforcement action confirms the conclusion that the FTC's May 2023 policy statement reflects a broad set of guidelines for companies that collect or use biometric information, and non-compliance may result in the FTC filing suit under Section 5 of the FTC Act. Accordingly, companies operating in the United States should consider reviewing their biometric information collection practices, employee training for handling biometric information, and contracts with vendors that process biometric information for compliance with the FTC's policy statement.