FTC's OkCupid/Match Case Signals Return to Section 5 Deception Complaints – With a New Twist on AI Disclosures

APRIL 3, 2026

D. REED FREEMAN JR., ANDREA M. GUMUSHIAN, MICHELLE R. BOWLING, JOHN M. KEBLISH

The Federal Trade Commission's (FTC) recent case against OkCupid and Match Group Americas is a classic FTC Section 5 deception action focused on false and misleading privacy promises about third-party data sharing, with the notable distinction that the third-party recipient was an artificial intelligence (AI) company.

The stipulated order bars future misrepresentations about data practices, underscoring a turn away from Biden/Kahn-era enforcement actions that pushed the boundaries of unfairness, while spotlighting AI disclosures as a must-have in privacy notices and vendor contracting. The clear takeaway is that companies need to ensure that their privacy disclosures accurately cover all third-party sharing, including AI platforms, and to put appropriate data processing agreements in place before any data flows. To the extent possible, avoid "we do not," "we never," and "we always" statements (and similar ones) unless you know for sure that they are true and will be until the next privacy policy update.

What the FTC Filed and Where the Case Stands

The FTC filed a single-count federal **complaint** in the Northern District of Texas alleging that Humor Rainbow, Inc. (which operates OkCupid) and Match Group Americas deceived consumers in violation of Section 5(a) by sharing user data with an unrelated third party contrary to OkCupid's privacy policy. The complaint seeks a permanent injunction and other equitable relief under Section 13(b). The FTC's

press release frames the case simply: OkCupid allegedly shared personal information, including photos and location, with an unrelated third party, contrary to their privacy promises.

The parties submitted a stipulated order for permanent injunction, which, upon court approval, will impose injunctive and compliance obligations for 10 years. The order focused on truthful disclosures about data practices and privacy controls for the OkCupid service and any online dating successor. The FTC's governing body vote to authorize filing the complaint and stipulated final order was 2–0 and is pending before the Northern District of Texas.

The Core Allegations: Privacy Promises vs. AI Vendor Access

The complaint alleges that OkCupid's privacy policies told users the company would not share "personal information with others except as indicated in this Privacy Policy or when we inform you and give you an opportunity to opt out," but nonetheless gave a third party without offering opt-out. The complaint alleges that the third-party data recipient did not fall into any disclosed category under OkCupid's privacy policy. The FTC asserts that in September 2014, the third party requested large datasets of OkCupid photos, and OkCupid's leadership facilitated access to nearly three million OkCupid user photos along with demographic and location information.

A central factual allegation is the lack of contractual governance. The complaint states that "Humor Rainbow never executed a formal agreement or set forth restrictions" on the recipient's access to or use of the data, and that the recipient provided no services and paid nothing in return. The complaint further alleges the companies took "extensive efforts to conceal and deny" the sharing, including public statements denying any involvement. Taken together, these facts present a traditional deception case grounded in divergence between policies and practices.

The Legal Theory: Classic Section 5 Deception, Not Novel Unfairness

---

The complaint asserts a single deception count under Section 5(a), alleging false and misleading claims about limits on data sharing and promised opt-out. The pleading does not pursue broader "unfairness" or expansive data-security theories; rather, it tracks the familiar pattern that a company represented it would confine sharing to enumerated categories and offer opt-out but did not. The FTC's press release reinforces that posture by quoting the Bureau of Consumer Protection Director: "The FTC enforces the privacy promises that companies make," and it will act when firms "promise to safeguard your data but fail to follow through."

For compliance, the case tees up a straightforward risk where marketing and policy statements might not match reality. This was not the FTC's attempt to stretch Section 5 around novel AI concepts. Rather, the alleged undisclosed transfer to a non-service provider AI company, with (also alleged) no notice, no opt-out, and no contractual limits, fits squarely within traditional deception doctrine.

The Proposed Order: Permanent Prohibitions and Long-Tail Compliance

The stipulated order prohibits misrepresentations from the defendants, express or implied, about:

- How they collect, maintain, use, disclose, delete, or protect personal information.
- The purposes for which they process personal information.
- The function of privacy controls, including consumer choices afforded under state privacy laws or other mechanisms the companies present to limit or manage processing.

These prohibitions align with the complaint and aim to ensure public-facing statements reflect actual practices across OkCupid and any successor dating service.

The order includes obligations to distribute the order to personnel, secure acknowledgments, and file a one-year compliance report under penalty of perjury, with continued notice of key changes for 10 years. Recordkeeping must cover privacy complaints and documents necessary to demonstrate compliance for a decade, with five-year retention per record. The FTC receives broad compliance monitoring rights, and the order remains in effect for 20 years from entry. Consistent with the deception posture, the relief is injunctive and compliance-focused rather than monetary.

What Is Distinctive Here: Third-Party AI Facial Recognition as the Data Recipient

The feature that will resonate across industries is that the third party was an AI technology company. This matters because many organizations now interact with AI platforms for analytics, content moderation, image or voice analysis, fraud detection, and other back-end or product-integrated use cases. A disclosure that says "we share data with service providers" often will not cover an unrelated AI vendor that is not a processor bound by a data processing agreement. Where a company's policy reserves sharing with specific categories, or commits to notice and opt-out before broader sharing, any transfer to an AI platform must either fit within a disclosed category or be separately disclosed with an opportunity to opt out if promised.

Practical Compliance Implications

The most immediate step is to reconcile your privacy notices with reality, with special attention to third-party disclosures involving AI platforms. If your current disclosures limit sharing to service providers and affiliates or commit to notice and opt-out for other transfers, but your teams upload or stream personal data to AI vendors outside those channels, your notice and practices are misaligned in ways that map directly onto the OkCupid allegations. The FTC framed this enforcement as "enforc[ing] the privacy promises that companies make," which is the classic lens through which it scrutinizes marketing and policy statements.

Contracting is just as critical. The complaint alleges that OkCupid "never executed a formal agreement or set forth restrictions" governing the AI company's access to, or use of, the data, and that absence is a central compliance failure. If an AI company receives personal information, companies should implement written agreements that define purpose, impose use restrictions, control retention and deletion, restrict downstream sharing, and require appropriate security, so they can accurately describe the relationship and rely on those controls when representing that a third party is acting as a service provider.

Enforcement Outlook: A Narrow Case With Wide-Reaching AI Disclosure Lessons

As alleged, this is a narrow case about privacy promises, not a novel theory about the inherent risks of AI or a new unfairness template. The complaint's single deception count and the order's misrepresentation prohibitions reflect a back-to-basics approach to Section 5. While the action does not chart new legal ground, it reiterates that the FTC will police privacy promises with particular attention to undisclosed AI data flows. For businesses, the lesson is not that AI is off-limits, but that AI-related sharing must be precisely disclosed and appropriately governed.

If you have any questions, please reach out to your ArentFox Schiff contact or a member of the **Privacy & Data Security** team.

Additional research and writing from Perry Jackson, law clerk in ArentFox Schiff's Washington, DC, office.

Contacts

D. Reed Freeman Jr.

PARTNER

Andrea M. Gumushian

ASSOCIATE

Michelle R. Bowling

SENIOR ASSOCIATE

John M. Keblish

ASSOCIATE

Related Practices

Privacy & Data Security

Continue Reading

PRIVACY COUNSEL

CIPA Plaintiffs Target Cookie Banners, Join State Regulators in Attack on Opt-Out Compliance

MARCH 31, 2026 | D. REED FREEMAN JR., ADAM D. BOWSER, ANDREA M. GUMUSHIAN, MICHELLE R. BOWLING, JOHN M. KEBLISH

PRIVACY COUNSEL

CalPrivacy Supports Bill Providing First-of-Its-Kind Incentives and Protections for Privacy Whistleblowers

FEBRUARY 27, 2026 | D. REED FREEMAN JR., ANDREA M. GUMUSHIAN, MICHELLE R. BOWLING, JOHN M. KEBLISH

PRIVACY COUNSEL

A New Era of US Privacy Enforcement Has Only Just Begun: 2025 Trends and Outlook for 2026 and Beyond

JANUARY 21, 2026 | D. REED FREEMAN JR., MICHELLE R. BOWLING, ANDREA M. GUMUSHIAN, JOHN M. KEBLISH

All Insights from Privacy Counsel