VENABLE LLP

FTC OkCupid Settlement: Deceptive Data Sharing, Privacy Policy Compliance, and Section 5 Takeaways

April 08, 2026

Rob Hartwell, Michael A. Signorelli and Kathryn Marshall Timmons

The FTC's Complaint: Alleged Deceptive Data Sharing and Privacy Policy Violations

As described in the complaint, OkCupid maintained for several years a privacy policy that stated the company did not share personal information other than with specific parties, including service providers, business partners, and businesses within its "family of businesses," for specific purposes.

However, the FTC alleged that OkCupid provided a third-party AI company-with which it had "no business relationship"-with access to information about millions of OkCupid users, such as photos, demographic information, and location information. The recipient, Clarifai, was not an entity with which the OkCupid privacy policy permitted the company to share data, according to the FTC. Rather, OkCupid's founders allegedly were financially invested in Clarifai, and Clarifai received the OkCupid user data without paying for such data, without agreements for the use of the data, or without providing services to OkCupid.

According to the FTC, by disclosing personal information to Clarifai in violation of the OkCupid privacy policy, OkCupid engaged in a deceptive act or practice in violation of Section 5 of the FTC Act. While sharing data with AI companies may be a relatively new practice, needing to maintain accurate privacy policies is not. For decades the FTC has warned that disclosing personal information in ways contrary to a company's privacy policy may be a deceptive act or practice in violation of Section 5 of the FTC Act.

The FTC Consent Order: Section 5 Restrictions and Evolving Privacy Enforcement Approach

Under the proposed 20-year consent order, OkCupid and Match would be prohibited from mispresenting the companies' information practices and the function of privacy controls or choices presented to consumers. In addition, the proposed consent order includes acknowledgment, compliance reporting, and recordkeeping requirements that are commonly imposed by FTC consent orders.

However, the order would not impose more affirmative obligations included in many prior FTC

consent orders, such as requiring companies to implement and maintain privacy programs or restrictions on specific practices. This action, along with those carried out in privacy-related cases under Chair Ferguson, may signal that the FTC is tailoring its approach to privacy settlements in a way that prior commissions did not.

Key Takeaways: Privacy Policy Compliance, Data Governance, and AI Data Sharing

Maintaining accurate privacy policy disclosures, and honoring what those disclosures say, has long been-and will continue to be-essential to a well-tuned data governance program. While growing state law requirements, new technologies, and other innovations may attract compliance resources, it is important to make sure the bedrock of your compliance program remains solid. Additionally, before engaging in new data practices, such as sharing with new partners or for AI training purposes, make sure your representations support that purpose.

If you have questions about FTC privacy enforcement trends, creating or testing data governance programs, or related developments, please reach out to Venable's Privacy and Data Security Group for assistance.