

DATA PRIVACY & GOVERNANCE HUB

MAC Lawsuit Raises Privacy Concerns Over AI Beauty Tools

JULY 29, 2026

Key Takeaways

- A class action lawsuit against MAC Cosmetics alleges its AI-powered beauty tool collected a consumer's biometric data without adequate disclosures or written consent.
- A federal judge denied MAC's motion to dismiss the suit, allowing the case to proceed due to the plaintiff's claim.
- The lawsuit highlights the need for explicit consumer consent when implementing AI-powered tools in the cosmetic industry.

What Happened

On June 4, a US federal judge in Illinois denied MAC Cosmetics' motion to dismiss a consumer's data privacy suit. This class action lawsuit arose from an Illinois resident, Fiza Javid, who claimed that MAC Cosmetics collected her facial geometry and biometric data through its in-store and online visual try-on [services](#) without proper disclosures or written consent.

In response to the claim, MAC disputed that the Biometric Information Privacy Act ([BIPA](#)) only encompasses biometric data capable of identifying an individual. The company asserted the consumer failed to demonstrate that the virtual try-on data could be used to identify her.

The case highlights concerns about the beauty industry's use of AI-powered [personalization](#) tools, which lead to the collection of biometric data, and a lack of informed consent.

Privacy and Governance Concerns

The AI-powered personalization tools, such as facial geometry and facial scans, are often used in the beauty industry, digital entertainment, and healthcare. As for the beauty industry, it allows [customers](#) to see how products may look on their faces without the need for physical [application](#). Brands such as Sephora, L'Oréal, and MAC have already implemented these technologies for in-store and online use.

Although such tools offer convenience, fun, and customer engagement, they also raise major concerns. Issues that arise are unauthorized collection and retention of sensitive biometric data, potential misuse or sharing, increased risk of identity-related privacy harms if information is compromised, and a lack of [transparency](#) about how long the data will be stored or who has access to it.

Additionally, such personalization tools that collect biometric data could be used to identify, track, or profile individuals. Even though MAC states it could not identify users from the technology alone, privacy advocates caution that biometric data may become identifiable when linked to other datasets. Biometric data is sensitive, especially since it cannot be changed if [compromised](#). This heightens concerns about how data is stored and the effects of a potential data breach.

Why It Matters / Policy Considerations

The MAC lawsuit raises major privacy concerns about AI-powered virtual try-on services. While Illinois's BIPA establishes strong privacy protections for Illinois [residents](#), not all states have fully adopted such [legislation](#). As AI-powered tools and techniques become more prevalent across the beauty industry, organizations may collect such sensitive data without proper consent, data retention, security, and deletion practices.

Enhancing oversight practices will require organizations to obtain consent before offering any virtual try-on services and to inform consumers how their data will be stored. Another appropriate oversight method could be the Federal Trade Commission ([FTC](#)), which could set strict guidelines and penalties if organizations fail to assess potential customer harm. Privacy advocates recommend clearer guidelines regarding consent requirements, transparency, [data](#) retention, and ensuring consumer privacy.