Bilzin Sumberg

EMERGENT LEGAL ISSUES IN THE TECH INDUSTRY | JUNE 2, 2026

Facial Recognition and the New Frontline of Data Sharing Liability

Kelly Ruane Melchiondo

The rapid integration of biometric technologies and facial recognition into commercial ecosystems is driving a new wave of privacy litigation, with regulators increasingly focused not only on data collection, but on the downstream, or "secondary," use of data for artificial intelligence training and analytics. Recent enforcement activity underscores a clear shift in regulatory posture: companies are no longer evaluated solely on whether they lawfully obtained user data, but also on whether subsequent uses align with disclosed purposes and reasonable consumer expectations. This shift is particularly acute in the biometric context, when companies convert photographs and facial data into persistent identifiers and deploy them across multiple systems. The results are heightened privacy risk and potential liability.

The Federal Trade Commission's March 2026 enforcement action against Match Group and its subsidiary OkCupid is instructive. There, the FTC alleged that OkCupid shared nearly three million user photos, associated demographic and geolocation data, with a third-party facial recognition company, without notifying users or providing them an opportunity to opt out. The agency emphasized that this conduct directly contradicted OkCupid's representations that it limited data sharing to others in defined categories, such as service providers and affiliates. The FTC alleged that, when it transferred data to an unaffiliated AI developer for model training purposes, OkCupid exceeded the scope of user consent and its disclosed practices.

The FTC framed the conduct as both deceptive and unfair under Section 5 of the FTC Act, highlighting that the case did not turn on the initial collection of user data—which users voluntarily provided—but rather, on the undisclosed secondary use of that data. This distinction is critical. Regulators are increasingly focused on "purpose limitation," meaning that even properly collected data can give rise to liability if a company later repurposes it in a manner inconsistent with its original disclosures. The complaint also highlighted OkCupid's alleged efforts to obscure its relationship with the third-party recipient once it became public, reinforcing the FTC's position that even a company's transparency failures, without more, can sustain deception claims.

OkCupid settled with the FTC. While the settlement lacked a monetary penalty, the FTC imposed meaningful injunctive relief. The FTC prohibited Match Group and OkCupid from misrepresenting how they collect, use, or share personal data—including biometric identifiers—and require them to implement ongoing compliance and reporting obligations. This is consistent with a broader enforcement trend in data privacy, cybersecurity AI-related privacy matters, in which regulators prioritize behavioral remedies, monitoring, and forward-looking compliance frameworks over purely financial penalties.

More broadly, the case illustrates how regulators and plaintiffs are leveraging traditional consumer protection laws, even in jurisdictions that do not specifically govern the use of biometrics, to police the expanding AI data supply chain. This creates a layered risk

environment in which the same conduct may trigger FTC scrutiny, state unfair trade practices claims, and privacy class actions for companies that fail to clearly disclose how they are using biometric data for AI development or sharing data with third parties.

For companies operating in the biometric space, even in jurisdictions that do not specifically regulate the use of biometric data, the potential for liability has expanded exponentially. Liability risk now extends beyond data collection to encompass the full lifecycle of data use, including AI model training, enrichment, and downstream commercialization. To mitigate risk, companies should implement robust data governance frameworks that include clear, granular disclosures beyond collection and primary use, transparent and wide-reaching consent mechanisms that contemplate and disclose AI-related uses, and continuous auditing and disclosure of data sharing across internal and external systems.

Related Practices

Data Privacy & Security | Technology | Commercial Litigation

Related People

Kelly Ruane Melchiondo

Partner, Construction, Trial & Litigation