wiley

NEWSLETTER

Facial Recognition Tech and Biometrics Under Scrutiny at FTC
—

February 2021

Privacy In Focus®

On January 11, 2021, the Federal Trade Commission (FTC) announced a proposed settlement with the photo storage and organization app developer Everalbum, Inc. (Everalbum) regarding its collection of biometric data and use of facial recognition technology. This proposed settlement is significant in showing the agency's developing approach to biometric privacy and use of facial recognition technology —which continue to draw interest from policymakers and regulators at both the federal and state level. The FTC's settlement provides some guidance for companies that collect biometric data and use it to train algorithms (including facial recognition), as a well as a clear warning that alleged privacy violations in this area will be treated seriously.

The Settlement Highlights the Critical Importance of Accurate Disclosures to Consumers When Biometric Privacy is Involved

The FTC's enforcement action against Everalbum centered on its "Ever" app—a cloud-based tool that allows users to upload photos and videos for storage and organization. The app included a "Friends" feature that used facial recognition technology to group photos together, and that also allowed users to tag people in their photos by name. The company also combined images it extracted from users of its "Ever" app with other images it got from publicly available datasets to help development its proprietary facial recognition technology, including technology that it ultimately marketed to other businesses through its enterprise brand. The company's privacy practices evolved from when it was first launched. Initially, it did not seek consumer consent. Then, for a period of time,

Authors
—

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas
—

FTC Regulation
Privacy, Cyber & Data Governance

it only sought consent from users in certain jurisdictions (such as Illinois, Texas, and Washington) that have biometric privacy laws requiring consent in certain circumstances. Eventually, according to the FTC, it offered all users a choice.

One of the FTC's core allegations against the company is that its representations to its users about their choices were inconsistent with Everalbum's practices. In particular, the FTC took a hard look at a "help" page on the company's website that discussed facial recognition that (it alleged) suggested that use of facial recognition was a choice for all consumers, at a time when consent was only obtained in limited jurisdictions. The FTC also alleged that, despite representing to consumers that the photos and videos would be permanently deleted when users deactivated their accounts, the company retained photos and videos indefinitely until recently changing its practices.

Like many privacy cases, the FTC's complaint was focused on alleged deception about privacy practices rather than how the data was used. At the same time, the complaint and settlement suggest unease and a closer look when biometric data and facial recognition technology in particular are involved. The FTC's complaint does not argue that the company's proprietary facial recognition technology—which it helped develop with user images—was used in a harmful fashion. Indeed, the complaint suggests that the technology was being used for routine purposes, such as access control and facilitating payments; it even acknowledges that Everalbum submitted the technology to the National Institute of Science and Technology (NIST) for accuracy testing. In effect, the FTC is signaling that misrepresentations about biometric data and facial recognition technology are itself sufficiently harmful to consumers to justify an enforcement action.

The Settlement Terms and Separate Statement Reinforce the Potentially Strict Penalties for Privacy Violations in Dealing with Facial Recognition and Algorithms

The proposed settlement—even though it does not include a monetary payment—would impose substantial penalties and restrictions on Everalbum. Of note, it would require the company to obtain affirmative express consent from users prior to extracting information from facial images or using biometric data to train, develop, or alter facial recognition technology—requirements that go beyond existing federal law. It would also require the company to destroy any models or algorithms developed in whole or in part from its users' biometric information.

The latter condition in particular shows the potentially far-reaching impact of the settlement. The company was required not only to destroy individual data it collected (not necessarily unusual in a privacy case), but also to *destroy proprietary algorithms based on the data.* As noted above, the FTC did not allege that the technology was itself misused. Rather, in his separate statement, Commissioner Chopra makes clear that this was a penalty "requiring [the company to] forfeit the fruits of its deception." In many cases, imposing such a remedy for a privacy violation may be even more burdensome for a company than a monetary payment. Indeed, it may not be a coincidence that the FTC is seeking this kind of remedy at the same time that its authority to seek monetary relief in similar cases is being challenged at the Supreme Court. And notably, the overall vote on these settlement terms was 5-0.

In his separate statement, Commissioner Chopra also states his position that "facial recognition technology is fundamentally flawed and reinforces harmful biases," and that he "support[s] efforts to enact moratoria or otherwise severely restrict its use." This view goes well beyond what the FTC itself has said about the technology, but reinforces that companies using biometric data and facial recognition technology will face scrutiny over their privacy approaches, at a minimum, in addition to potential issues concerning algorithmic bias. Companies that collect or use biometric data or that utilize facial recognition technology already face a complex regulatory landscape (particularly at the state level), and compliance with evolving FTC expectations will be important going forward.