Cooley

# FTC Requires App Developer to Obtain Users' Express Consent for Use of Facial Recognition

January 19, 2021

The Federal Trade Commission announced on January 11 that Everalbum, the developer of the photo storage application called Ever, settled allegations that it deceived users about its use of facial recognition technology and retained photos and videos from users who had deactivated their accounts in violation of its own privacy policy.

Everalbum agreed in the settlement to (1) obtain users' express consent before using facial recognition technology on users' photos and videos, (2) delete or destroy all facial recognition data collected from users who have not provided consent, (3) delete or destroy the photos and videos of deactivated accounts and (4) notably, to delete models and algorithms that Everalbum developed using the photos and videos uploaded by users.

The settlement sends a clear message that the FTC will continue to focus on the privacy issues implicated by the collection of biometric data, including through the use of facial recognition. Andrew Smith, Director of the FTC Bureau of Consumer Protection, stated, in announcing the settlement, "ensuring that companies keep their promises to customers about how they use and handle biometric data will continue to be a high priority for the FTC."

FTC settlements often lead to follow-on litigation – including expensive and burdensome consumer class actions. Thus, tech companies, big and small, should be on notice that the collection and use of biometric data is facing increasing legal risk and they need to adhere to their privacy policies.

The FTC's focus on biometric data further means that companies need to implement robust privacy compliance programs governing their processing of biometric data in all facets of their business operations – from product development to consumer engagement.

## FTC's allegations of misuse of facial recognition

According to the FTC, the Ever app, launched in 2015, allowed users to upload and store photos and videos to its cloud servers. In February 2017, Everalbum added a "Friends" feature to the app. The feature used facial recognition to group users' photos by faces that appear in the photos. It also allowed users to apply "tags" to identify the people who appear in their photos.

### Alleged misrepresentations of choice and consent

The FTC alleged that even though between 2017 and 2019 the Ever app did not give most users the choice to consent to the use of facial recognition technology on their photos, Everalbum misled consumers into thinking that the facial technology would not be used without their affirmative express consent. The FTC zeroed in on the "Help" section of Everalbum's website, which explained that, "when face recognition is turned on, you are letting us know that it's ok for us to use the face embeddings of the people in your photos and videos, including you, and that you have the approval of everyone featured in your photos and videos." According to the FTC, it was not until 2019, that Everalbum gave all users the ability to disable and enable facial recognition.

The FTC alleged that in spite of that commitment, when the Ever app launched the Friends feature in 2017, it enabled facial recognition by default for all app users and did not provide an option to disable it. Between May of 2018 and 2019, Everalbum implemented consent mechanisms, but only for users in jurisdictions with specific biometric privacy laws – Illinois, Texas, Washington and the European Union – who received the option to disable and enable the facial recognition feature.

The FTC further alleged that Everalbum began developing its own facial recognition technology and used

images it extracted from the Ever app's users' facial images to improve the technology. Everalbum combined users' facial images uploaded to the app with facial images obtained from publicly available sources to create datasets. Everalbum then used the resulting facial recognition technology both in the app and to build the facial recognition services that its enterprise brand, Paravision (formerly Ever AI), offered to business customers.

**Alleged misrepresentation of data retention practices**

The FTC also alleged that at least until October 2019, Everalbum deceived users about what would happen to their photos and videos after accounts were deleted. Despite representing that Everalbum would delete users' photos and videos if they deactivated their accounts, the FTC alleged that the company instead retained user data.

# FTC proposed order

The FTC's proposed order, which the commissioners voted unanimously to accept, requires Everalbum to:

1. provide notice and obtain affirmative express consent before using biometric information in connection with facial recognition technology;
2. delete or destroy the photos and videos of deactivated accounts;
3. delete or destroy models or algorithms that Everalbum developed in whole or in part using biometric information that the Ever app collected from its users; and
4. delete or destroy facial recognition data collected from users who had not provided express affirmative consent.

The order also prohibits Everalbum from misrepresenting how it collects, uses, discloses, maintains or deletes personal information.

Requiring Everalbum to delete its models and algorithms is an aggressive step for the FTC, which, according to Democratic FTC Commissioner Rohit Chopra in his separate statement, "previously voted to allow data protection law violators to retain algorithms and technologies that derive much of their value from ill-gotten data."

While the FTC did not impose any monetary fine or penalty, this might change in the future. Chopra criticized the lack of monetary penalties, stating that, "the FTC needs to take further steps to trigger penalties, damages and other relief for facial recognition and data protection abuses." Companies can expect that the FTC in the future will push for such monetary remedies, pending Supreme Court review as to whether the FTC Act empowers the FTC to seek monetary damages, in addition to injunctive relief.

While the FTC awaits the Supreme Court's decision, Congress may well provide new statutory authority. In September 2020, four Republican senators introduced S. 4626, the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act. That legislation, among other things, would strengthen the FTC's enforcement authority by clarifying the FTC's ability to obtain monetary remedies. The groundwork is set for further action in 2021 by a Democrat-controlled 117th US Congress.

# Takeaways for companies

The settlement is a reminder that companies whose core products rely on models and algorithms should ensure that such models and algorithms do not rely on deceptively or otherwise wrongfully collected data. The Everalbum enforcement action sets a significant precedent that could result in the loss of those core products should companies find themselves in the FTC's crosshairs.

The enforcement action also serves notice to companies that they will need to be especially careful in complying with privacy requirements when deploying facial recognition technology, which privacy advocates, legislators and regulators view as highly sensitive.

Facial recognition technology has indeed already emerged as a high-profile issue for privacy advocates, who have argued that such technology has the potential to infringe on privacy rights. For example, the Electronic Privacy Information Center frequently files complaints with the FTC urging agency action.

Some privacy experts have also expressed concerns about racial bias in facial recognition algorithms, as such artificial intelligence and related technologies have gained widespread use. The incoming Biden administration has also noted potential problems with such technologies, particularly as it relates to racial bias and criminal justice. Commissioner Chopra, in his separate statement, in fact argued that in the future, "it will be critical for the Commission, the states, and regulators around the globe to pursue additional enforcement actions to hold accountable providers of facial recognition technology who make false accuracy claims and engage in unfair, discriminatory conduct."

Facial recognition technology has also become a popular target for class action litigation under the Illinois Biometric Information Privacy Act (BIPA), which created significant liability exposure for companies that utilize facial recognition in their operations, along with other statutes. In May 2020, for example, the American Civil Liberties Union sued a facial recognition firm for violations of BIPA, alleging the company unlawfully collected and used biometric data without providing notice or obtaining consent from Illinois residents, and then sold access to its technology to law enforcement and private firms.

Given this increased legal scrutiny, companies that deploy facial recognition technology and other technologies to collect and use biometric data should consider the following best practices:

- **Implement privacy-by-design.** Companies should consider privacy in the entire product development lifecycle, including understanding the purposes of data collection, the types and amount of data collection the product requires, data retention minimization and the building of technology to enable consumer choice.
- **Implement transparency and choice.** If a company collects biometric data, it should provide in-time notice to those individuals and must give them a meaningful choice about the collection that is easy for consumers to exercise. For companies collecting biometric data through mobile applications, notice and choice should be provided at the point of installation of the application or in-time in the user journey.
- **Consult with legal counsel.** Companies should ensure that any notice, policy, consent forms and information security programs comport with applicable laws regarding the use of biometric data.
- **Ensure continuing accuracy of privacy-related representations.** Significantly, the FTC's misrepresentation allegations focus on a statement that Everalbum made in the "Help" section of its website, making it imperative that companies closely review and monitor public-facing statements to ensure that any material representations regarding privacy and cybersecurity accurately reflect the company's data practices. Companies should regularly assess compliance with the privacy and information promises on their website and applications, as well as in other advertising and social media posts, to ensure that representations regarding privacy and cybersecurity accurately reflect their data practices.



# Key Contacts


| | |
|---|---|
| Dee Bansal<br>Washington, DC | dbansal@cooley.com<br>+1 202 728 7027 |

| | |
|---|---|
| Howard Morse<br>Washington, DC | hmorse@cooley.com<br>+1 202 842 7852 |