

Everalbum Settles FTC Claims Alleging Deceptive Use of Facial Recognition Technology

The first-of-its-kind settlement suggests that the FTC and other regulators will scrutinize facial recognition technology.

What Happened?

The Federal Trade Commission (FTC) [announced](#) on January 11, 2021, that it had reached a [settlement](#) with Everalbum, Inc., the developer of a now-defunct photo storage app called "Ever." The settlement is the FTC's first enforcement action focused on facial recognition technology, and likely signals a new era of increased regulatory scrutiny for companies involved in facial recognition. It provides for broad relief, including the unprecedented requirement that Everalbum delete "any models and algorithms" based on any "[b]iometric [i]nformation" collected from users of the Ever app. The settlement is also likely to inspire more private lawsuits focused on how companies use and describe facial recognition technologies.

Background. Everalbum's Ever app allowed users to store and organize their digital photos and videos by uploading them to Ever's cloud-based servers. According to the FTC's administrative [complaint](#), Ever launched a new feature—called "Friends"—in 2017. The Friends feature used facial recognition technology to group users' uploaded images based on similarities among faces that appeared in the images.

The Complaint. The gist of the FTC's complaint is that Everalbum deceived users about the Ever app's use of facial recognition technology and thereby violated Section 5 of the Federal Trade Commission Act, which prohibits "deceptive acts or practices in or affecting commerce." Specifically, the FTC alleges that Everalbum deceived users by:

- Promising to delete users' images if users deactivated their accounts but, in fact, retained images associated with deactivated accounts "indefinitely" between 2017 and October 2019.
- Publishing an article in the "help" section of its website suggesting that Ever would apply facial recognition technology to users' images only if users consented—even though that was true only for some users, some of the time.

The second allegation requires explanation. According to the FTC, Everalbum gave different users different levels of control over facial recognition technology at different times depending on where they were located. Beginning in May 2018, users in Texas, Illinois, Washington, and the European Union were given the opportunity to opt in to the use of facial recognition technology in the Ever app and were also given the ability to turn the technology on and off. (Notably, all those jurisdictions have laws governing biometric data.) In contrast, until April 2019, users outside those jurisdictions were not given the opportunity to opt in to the use of facial recognition technology—rather, the technology was "enabled" by "default"—and they were not able to turn the technology on and off. Thus, the FTC concluded that Everalbum's help center article suggesting that Ever used facial recognition technology only with consent was "misleading for Ever mobile app users located outside of Texas, Illinois, Washington, and the European Union" before April 2019.

The Settlement. If approved by the FTC after a public comment period, the parties' settlement will provide for the following relief:

- Everalbum will be prohibited from misrepresenting how it collects, retains, and uses personal information, including but not limited to facial recognition-related information.
- Everalbum will be required to obtain affirmative express consent (i.e., clear and conspicuous notice and opt-in consent) from users before collecting "biometric information" for certain purposes.
- Everalbum will be required to delete photos and videos of Ever app users who requested deactivation of their accounts.
- Everalbum will be required to delete "face embeddings"—i.e., "data . . . derived in whole or in part from an image of an individual's face"—based on images of Ever users who did not consent to the creation of the face embeddings.
- Everalbum will be required to delete "any models or algorithms" developed using biometric information from images of Ever app users.

The last remedy is notable for two reasons. First, it appears to be unprecedented in the history of FTC settlements. Although FTC settlements often require the deletion of the data that the FTC alleged had been collected unlawfully, this is the first time, to our knowledge, that the FTC has required a company to delete the algorithms or other work product incorporating data that was (allegedly) collected improperly. Second, although the FTC's complaint includes allegations suggesting that Everalbum developed its facial recognition technology with improperly obtained data, it does not include a claim based on those allegations. While the FTC often prohibits more than the allegedly unlawful conduct in its orders for the sake of "fencing in" an alleged wrongdoer, it is unusual for such "uncharged" conduct to be discussed at length, if at all, in the FTC's complaint, or for it to comprise such a significant component of the remedy.

The settlement does not include any monetary relief. The FTC lacks authority to obtain civil penalties for Section 5 violations, and its authority to obtain equitable monetary relief, such as restitution or disgorgement of ill-gotten gains, is under review by the U.S. Supreme Court. However, violations of the settlement, once finalized, can lead to maximum penalties of more than \$43,000 per violation.

Chopra Statement. In a separate [statement](#) issued at the same time the Everalbum settlement was announced, FTC Commissioner Rohit Chopra argued that "[t]oday's existing facial recognition technology is fundamentally flawed and reinforces harmful biases," and that the "case of Everalbum is a troubling illustration of just some of the problems with facial recognition." He heralded the settlement for requiring Everalbum to "forfeit the fruits of its deception," that is, "facial recognition technologies enhanced by any improperly obtained photos," contending that earlier FTC settlements with other companies allowed those companies to "retain algorithms and other technologies enhanced by illegally obtained data." At the same time, Commissioner Chopra called the settlement's lack of a financial penalty "unfortunate" and reiterated his call for the FTC to "take further steps to trigger penalties, damages, and other relief for facial recognition and data protection abuses" in the future, such as by engaging in a rulemaking under Section 18 of the FTC Act.

Why Does It Matter?

There are several significant takeaways from the Everalbum settlement.

1. Increased regulatory scrutiny. The settlement strongly signals that the FTC is now focused on facial recognition and—most likely—biometric data-based technology more generally. While the FTC has addressed issues related to facial recognition in the past, including in a [2012 report](#), this is the first FTC enforcement action

focused principally on facial recognition technology. The press release announcing the settlement declares that it will be a "high priority" for the FTC to ensure that companies "keep their promises to customers about how they use and handle biometric data." In addition, the incoming Biden administration has announced its intention to nominate Commissioner Chopra to serve as the director of the Consumer Financial Protection Bureau (CFPB). In light of Commissioner Chopra's strongly expressed views in this case, he may steer the CFPB to scrutinize consumer financial products and services that incorporate biometric technology.

2. Stiff and broad requirements. The requirements imposed on Everalbum starkly illustrate the potential risks of regulatory enforcement. For example, as explained above, the settlement would not just require Everalbum to delete all facial recognition data collected without consent; it would also require Everalbum to delete all models and algorithms based on data collected from Ever users. For some companies, "unwinding" their use of facial recognition data in that way could be extremely disruptive and burdensome and could even represent an existential threat to their businesses. Equally important, the settlement would require Everalbum to provide notice and obtain opt-in consent before collecting and using biometric data for certain purposes—and it would require Everalbum to comply with those requirements everywhere the order applies, not just in the few jurisdictions that have already enacted laws with similar requirements

3. Broad use of deception authority. The Everalbum case reinforces that the FTC often uses its deception authority in the privacy arena against conduct it finds problematic even when there is no apparent intent to deceive, and even when the allegedly misleading statements appear only in secondary materials, such as help center articles. The FTC shied away from using its unfairness authority in this case, as it often does—perhaps out of concern it could not demonstrate the requisite consumer injury. But that restraint may have no practical significance because of the agency's broad use of its deception authority to reach conduct it finds problematic in the privacy sphere.

4. Potential for more state-level enforcement and regulation. The Everalbum settlement will likely encourage increased regulatory scrutiny of facial recognition technology and other biometric data-based technologies at the state level, as well. Most states have laws similar to Section 5 of the FTC Act. And it is common for state regulators to take their enforcement cues from the FTC. Commissioner Chopra's separate statement also encourages state legislatures to more strictly regulate biometrics, as Illinois, Texas, and Washington do. And that call is likely to be heeded. Many states, including New York, are actively considering new legislation to govern biometric data. And Portland, Oregon recently became the [first jurisdiction to ban the use of facial recognition technology](#) by private entities in places of public accommodation (with limited exceptions).

5. More lawsuits may be coming. The FTC settlement may increase companies' exposure to private lawsuits, including class actions. Private plaintiffs may point to the FTC settlement to try to support allegations that other companies' statements about their uses of facial recognition technology are deceptive, unlawful, or unfair under state consumer protection laws and similar laws. The settlement could also figure in current and future litigation under the Illinois Biometric Information Privacy Act (BIPA), which is the only state law governing biometric privacy that includes a private right of action. BIPA has already spawned nearly 900 putative class action lawsuits in recent years. And, as noted above, it is possible that the FTC settlement and Commissioner Chopra's calls for increased state-level regulation will inspire more jurisdictions to enact legislation specifically governing biometric data, including legislation that allows private parties to sue for violations.

What's Next?

The FTC's complaint and settlement will be published in the Federal Register and subject to public comment for 30 days, after which time they will very likely be approved by the FTC.

What Should I Do Now?

All companies that use or rely on biometric technology in their businesses should consult with experienced counsel to determine how the Everalbum settlement impacts them. Perkins Coie's experienced team has deep experience advising clients on facial recognition technologies and other types of biometric technologies, litigating cases relating to biometric data, and representing companies in FTC investigations. For further information, please send a message to biometrics@perkinscoie.com or contact one of the authors.

© 2021 Perkins Coie LLP

Authors



[Janis Kestenbaum](#)

Partner

JKestenbaum@perkinscoie.com



[Nicola Menaldo](#)

Partner

NMenaldo@perkinscoie.com [206.359.8000](tel:206.359.8000)



[Ryan Spear](#)

Partner

RSpear@perkinscoie.com [206.359.3039](tel:206.359.3039)



Susan Fahringer

Partner

SFahringer@perkinscoie.com [206.359.8687](tel:206.359.8687)



Debra R. Bernard

Of Counsel

DBernard@perkinscoie.com [312.324.8559](tel:312.324.8559)

Explore more in

[Technology Transactions & Privacy Law](#) [Privacy & Security](#) [Artificial Intelligence & Machine Learning](#)
[Communications](#)

Related insights

Update

Employers and Immigration Under Trump: What You Need To Know

Update

'Tis the Season... for Cybercriminals: A Holiday Reminder for Retailers