



FTC BREAKS NEW GROUND ON RETENTION OF INTELLECTUAL PROPERTY AND DATA IN *EVERALBUM* SETTLEMENT

by Jason D. Haislmaier and Paul B. Sudentas

Earlier this year, the U.S. Federal Trade Commission (FTC) announced that it reached a settlement in its enforcement action against Everalbum, Inc. (Everalbum), the developer of the “Ever” application (*In the Matter of Everalbum and Paravision*, Commission File No. 1923172). The settlement appears to be the first in which the FTC required the deletion of intellectual property developed using data obtained in violation of Section 5(a) of the Federal Trade Commission Act (Act), in addition to the data itself. In particular, the settlement requires that Everalbum delete all “Affected Work Product,” defined as “any models or algorithms developed in whole or in part using Biometric Information [Everalbum] collected from Users of the ‘Ever’ mobile application.”

The Ever App and the FTC Complaint. Launched in 2015, the Ever app allowed users to store and organize digital photos and videos from multiple sources using the app’s cloud-based servers. In February 2017, Everalbum launched a new feature—“Friends”—which used facial recognition technology to organize photos. Facial recognition was automatically enabled as a default for all users without any initial consent. Through the app’s “Help” page, Everalbum represented it would not apply facial recognition technology unless users affirmatively enabled the feature.

As of May 2018, Ever app users from Texas, Illinois, Washington, or the European Union (*i.e.*, places with laws regulating biometric information) had an option to allow the app to use facial recognition, including a setting that allowed those users to turn on/off the facial recognition feature. In April 2019, Everalbum made these same options available for users outside of those locations.

In its Complaint, the FTC asserts two primary counts of misrepresentation against Everalbum: (1) not using face recognition unless the user enabled it or turned it on; and (2) deletion of users’ photos and videos upon account deactivation. According to the Complaint, Everalbum used the images it extracted from users’ photos to develop and improve its facial recognition technology.

The FTC Settlement. The FTC settlement includes a number of now standard requirements regarding ceasing prior misrepresentations and making clear disclosure of information-sharing practices. However, the Everalbum settlement also breaks new ground in requiring that Everalbum:

- delete/destroy all “face embeddings”¹ derived from biometric data collected without express consent; and
- delete/destroy its work product derived from the use of users’ biometric information.

¹ “Face Embeddings” is defined as data derived in whole or in part from an image of an individual’s face.

Jason D. Haislmaier is a partner in the Boulder, CO office of Bryan Cave Leighton Paisner LLP, and **Paul B. Sudentas** is an associate in the firm’s New York, NY office.

This appears to be the first time that the FTC has required deletion of work product derived from ill-gotten data.

Implications of the FTC's Requirement to Delete Work Product. In requiring Everalbum to delete the facial recognition technologies enhanced by improperly obtained facial recognition data, the settlement moves beyond prior FTC settlements which only affected ill-gotten data itself. In doing so, the FTC appears to reiterate its longstanding position that compliance must be done at inception otherwise one must forfeit the “fruits of its deception.”

However, the deletion requirement also leaves questions unanswered concerning its effect on intellectual property rights. For example, (1) does the deletion requirement actually “destroy” intellectual property rights or merely the implementation of those rights?; (2) does the deletion requirement extend to models and algorithms derived from ill-gotten covered information that is *not* considered biometric information?; and (3) is Everalbum prevented from re-implementing its models and algorithms using properly obtained data?

While these questions remain to be answered, *Everalbum* makes clear that companies seeking to obtain and use biometric or other sensitive data should focus on providing and documenting proper notice, adhering to existing policies, and obtaining appropriate consent from users. While failing to do so has long had implications in the eyes of the FTC, it appears *Everalbum* has upped the stakes for those companies that fail to do so.