

**Insights****FTC SAYS THAT ONE CANNOT RETAIN THE FRUIT OF THE TAINTED TREE**

Mar 17, 2021

**SUMMARY**

Setting new precedent in the world of data, the FTC has found that the work product of ill-gotten data is no longer retainable by the developer. On January 11, 2021, 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” photo storage application (*In the Matter of Everalbum and Paravision*, Commission File No. 1923172). While the FTC has entered into dozens of such settlements over the prior two decades, the Everalbum settlement is unique as it appears to be the first settlement in which the FTC has required the deletion of intellectual property developed using data obtained in violation of the Federal Trade Commission Act (Act), in addition to the data itself. In particular, and in addition to requirements commonly seen in other FTC settlements (including broad notice, consent, and deletion requirements), the Everalbum 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 Used of the ‘Ever’ mobile application.” This settlement is likely to cause greater scrutiny of data subject consents and the collection of biometric information, and potentially impacts the collection of other sensitive personal information as well.

**The FTC’s Complaint**

In its complaint against Everalbum (Complaint), the FTC alleges that Everalbum violated Section 5(a) of the Act, which prohibits “unfair or deceptive acts or practices in or affecting commerce.” It consists of two primary counts:

1. Everalbum misrepresented that it was not using face recognition unless the user enabled it or turned it on.
2. Everalbum misrepresented that it would delete the users’ photos and videos upon deactivation of their accounts.

Notably, neither count is directed to the development of technology using data collected from the Ever app.

**Everalbum and the Ever App**

Launched in 2015 as a “free” app, the Ever app allowed users to store and organize their digital photos and videos from mobile devices, computers, social media accounts, or cloud-based storage service accounts by uploading them to the app’s cloud-based servers. In February 2017, Everalbum launched a new feature in the Ever app, called “Friends,” which used facial recognition technology to organize photos based on the faces of people who appear in the photos. At the launch of the Friends feature, facial recognition was automatically enabled as a default for all users of the Ever app without providing an initial option for consent. Through the app’s “Help” page, however, Everalbum represented that it would not apply its facial recognition technology unless users affirmatively enabled the feature.

As of May 2018, Everalbum gave Ever app users from Texas, Illinois, Washington, or the European Union an option to allow the Ever app to use facial recognition, including a setting that allowed those users to turn on or off the facial recognition feature. Notably, these locations have laws regulating the use of biometric information. In April 2019, Everalbum made these same options available for users outside of Texas, Illinois, Washington, and the European Union.

According to the Complaint, Everalbum used the images it extracted from the Ever app users’ photos to develop to improve its own facial recognition technology that it sold through Paravision—Everalbum’s enterprise brand.

**Settlement with the FTC**

The settlement, if approved by the FTC after the public comment period, does not include any civil penalties or monetary damages. It does, however, provide for significant relief against Everalbum concerning information from or about an individual consumer including, among other things, biometric information (defined in the Complaint as “Covered Information”):

- Everalbum shall not misrepresent:

- how it collects, uses, discloses, maintains or deletes Covered Information;
  - how users can control collection, use, disclosure, maintenance or deletion of Covered Information;
  - how it accesses users' Covered Information or how it permits users' access thereto;
  - how long it retains Covered Information after a user's deactivation of his or her account; and
  - how it protects privacy, security, availability, confidentiality, or integrity of Covered Information.
- Everalbum shall "clearly and conspicuously" disclose to the user the purposes for which Everalbum will use and share biometric information collected and shall obtain users' affirmative express from the user before collecting biometric information for development of new facial recognition technology.
  - Everalbum shall, within 30 days after the settlement issues, delete or destroy all photos and videos of users who requested deactivation of their accounts on or before the issuance date of the settlement.

Notably, and in a first of its kind maneuver, the Complaint also reaches beyond just Covered Information to require the deletion of intellectual property Everalbum derived from the Covered information:

- Everalbum shall, within 90 days after the settlement issues, delete or destroy all "face embeddings"<sup>1</sup> derived from biometric information collected from users who have not provided affirmative express consent for the creation of such "face embeddings."
- Everalbum shall delete or destroy its work product—e., models and algorithms—derived from the use of users' biometric information.

Although the Everalbum settlement falls largely in line with prior FTC precedent in requiring deletion of ill-gotten data, this appears to be the first time that the FTC has required deletion of work product derived from that ill-gotten data.

## Implications of FTC's Requirement to Delete Work Product

In requiring Everalbum to forfeit the "fruits of its deception,"<sup>2</sup> and delete the actual facial recognition technologies enhanced by its improperly obtained facial recognition data, the Everalbum settlement moves into new territory, beyond prior FTC settlements which only affected ill-gotten data itself while allowing companies to retain algorithms and other technologies derived from that data. While the FTC's action in Everalbum is squarely focused on the sensitive nature of the facial imagery and facial recognition data collected by the Ever app, the FTC has long identified other forms of "sensitive" information that it expects to be similarly treated.<sup>3</sup> Whether the new remedy seen in the Everalbum action remains limited to facial data or signals the start of a new trend in future FTC enforcement actions remains to be seen. However, the Everalbum settlement clearly presents important guidance for companies collecting and processing [sensitive] personal information.

In *Everalbum*, the FTC can be seen to reiterate its longstanding position that a mistake on the front end requires removal of any benefits on the back end. That is, compliance must be done at inception otherwise one cannot reap the spoils of the forbidden fruit. With the increased penalty for failing compliance, namely deletion of intellectual property, this settlement heightens the importance of attention to detail when obtaining consent, particularly with respect to sensitive information.

In addition, the new deletion requirement seen in *Everalbum* leaves substantial questions unanswered with respect to its effect on intellectual property rights, for example:

- Does the FTC's deletion requirement actually "destroy" intellectual property rights (*g.*, copyright and patent rights)? That is, following deletion of copyrighted models or software-implemented algorithms, is an entity still permitted to enforce its copyright in those models and software? Likewise, if the entity has obtained patents covering its deleted software, does the settlement have any effect on the validity or enforceability of those patents?
- While the deletion requirement is directed to ill-gotten biometric information, what about models and algorithms derived from ill-gotten covered information that is *not* considered biometric information?
- Going forward, is the entity prevented from re-implementing its models and algorithms using properly obtained data? If so, what steps must be taken to insulate the new models from those subject to deletion (*g.*, a "clean room" or similar process)? How different must the new work product be as compared to the work product that fell under the deletion requirement? And, can the entity simply recreate its work product verbatim using properly obtained data?

While these questions remain unanswered, what is clear from the *Everalbum* settlement is that, going forward, companies seeking to obtain and use biometric data (and likely other sensitive information) from data subjects should focus on providing and documenting proper notice, adhering to existing policies, and obtain 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.

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

2. *See*

[https://www.ftc.gov/system/files/documents/public\\_statements/1585858/updated\\_final\\_chopra\\_statement\\_on\\_everalbum\\_for\\_circulation.pdf](https://www.ftc.gov/system/files/documents/public_statements/1585858/updated_final_chopra_statement_on_everalbum_for_circulation.pdf)

3. *See, e.g.*, <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>

## RELATED PRACTICE AREAS

- Data Privacy & Security
- Start-Up & Venture Capital Practice

## MEET THE TEAM



**Jason D. Haislmaier**

Boulder

[jason.haislmaier@bclplaw.com](mailto:jason.haislmaier@bclplaw.com)

[+1 303 417 8503](tel:+13034178503)



**Christian M. Auty**

Chicago

[christian.auty@bclplaw.com](mailto:christian.auty@bclplaw.com)

[+1 312 602 5144](tel:+13126025144)



**Paul B. Sudentas**


New York

[paul.sudentas@bclplaw.com](mailto:paul.sudentas@bclplaw.com)

[+1 212 541 2009](tel:+12125412009)

---

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon ([kathrine.dixon@bclplaw.com](mailto:kathrine.dixon@bclplaw.com)) as the responsible attorney.

 Cookiebot session tracker icon loaded