Professional Perspective

AI/ML Algorithms Based on Impermissible Data Risk Deletion

Ken Kumayama and William Casey, Skadden, Arps, Slate, Meagher & Flom LLP

Bloomberg
Law

AI/ML Algorithms Based on Impermissible Data Risk Deletion

Contributed by Ken Kumayama and William Casey, Skadden, Arps, Slate, Meagher & Flom LLP

The use of artificial intelligence and machine learning to develop models and algorithms (AI/ML models) is now ubiquitous across a variety of industries. While much focus has been placed on what data is used to train AI/ML models, and what effects and biases may be caused through the use of AI/ML models, less attention has been paid to what result should occur if data is impermissibly used to train AI/ML models. Should a company be required to delete the data but be allowed to maintain models and algorithms that do not themselves contain such data? Or should the company also be required to delete AI/ML models that were created using the data?

Recently, in *In the Matter of Everalbum and Paravision*, the Federal Trade Commission issued a proposed consent order that has been unanimously approved by the FTC's commissioners, requiring Everalbum, Inc. not only to delete data taken and used impermissibly, but also – in contrast to prior orders – to delete any AI/ML models "developed in whole or in part" using such data.

Background

Beginning in 2015, Everalbum operated a photo storage and organization application called "Ever," which allowed users to upload photos and videos to Ever's cloud servers. In February 2017, Everalbum added a "Friends" feature that used facial recognition to organize users' photos based on the faces of the people who appear in them. When Everalbum added this feature, facial recognition was enabled by default and users did not have an option to turn off or disable the feature.

Beginning in May 2018, Everalbum provided a pop-up message to users in Texas, Illinois, Washington and the European Union asking them whether they would like Ever to use facial recognition technology to automatically create albums. The Friends feature and facial recognition were disabled for the users until they clicked "Yes," and users in those territories were given the option to turn the facial recognition feature on or off.

In July 2018, an article posted in the "Help" section of the Everalbum website stated that "[w]hen face recognition is enabled, the technology analyzes the photos and videos that you upload" and "[w]hen 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."

Nevertheless, it was not until April 2019 that users outside of Texas, Illinois, Washington and the European Union were presented with a pop-up message and default privacy settings similar to those provided to the users in those territories nearly a year earlier.

In developing its own facial recognition technology, Everalbum combined millions of facial images between September 2017 and August 2019 that it extracted from Ever users' photos with facial images that it obtained from publicly available datasets to create four datasets that it used in the development of its facial recognition technology.

In each of the datasets, Everalbum used computer scripts to identify and compile from Ever users' photos facial images that met all of the following criteria:

- not associated with a deactivated Ever account
- not blurry
- not too small
- not a duplicate of another image
- associated with a specified minimum number of images of the same tagged identity
- in three of the four datasets, not identified by Everalbum as being an image of someone under the age of 13

In a second dataset, compiled in April 2018, in addition to the six base criteria above, Everalbum excluded facial images extracted from photos of Ever users believed, based on their IP addresses, to be residents of either the U.S. or the European Union.

In June 2018, Everalbum compiled a third dataset that applied the same six base criteria as the other datasets and, in addition, excluded facial images extracted from photos of Ever users believed, based on their IP addresses, to be residents of Illinois, Texas, Washington or the European Union. Everalbum submitted the facial recognition AI/ML model derived from this third dataset to the National Institute of Science and Technology for accuracy testing and comparison to competing facial recognition technologies.

In August 2019, Everalbum compiled a fourth dataset that applied the same six base criteria as the other datasets and, in addition, excluded facial images extracted from photos of users who had neither turned on the facial recognition feature nor clicked "Yes" to the pop-up message described above (i.e., had not affirmatively consented to such use).

Everalbum used the facial recognition AI/ML model derived from this fourth dataset in Ever and to build facial recognition services offered by its enterprise brand, Paravision, which offers facial recognition technology to enterprise customers for purposes such as security, access control, and facilitating payments.

Prior to October 2019, Everalbum also had a privacy policy and sent account deactivation messages indicating that a user's data would be permanently deleted as soon as possible once an account was deleted. However, prior to October 2019, Everalbum retained indefinitely the photos and videos of Ever users who had deactivated their accounts. It was not until October 2019 that Everalbum began deleting all photos and videos associated with Ever accounts that had been deactivated for more than three months.

The FTC investigated Everalbum's actions and on Jan. 11, 2021, issued an agreement containing consent order that provided, in relevant part, that Everalbum: (1) prior to creating numerical representations of faces or training, developing or altering any facial recognition model or algorithm must (A) clearly and conspicuously disclose to the user, separate and apart from any privacy policy or terms of use, all purposes for which Everalbum plans to use or share such information and (B) obtain affirmative express consent from the user to do so; and (2) delete or destroy (A) all photos and videos of users that previously requested deactivation of their Ever accounts; (B) all data taken from users that do not provide express affirmative consent described in (1)(A) within 90 days; and (C) any models or algorithms developed in whole or in part using biometric information that Everalbum collected from users.

Analysis

The Everalbum consent order contains a first for the FTC—a requirement to delete AI/ML models created using wrongfully acquired or misused data. As noted by the statement of FTC Commissioner Rohit Chopra filed concurrently with the Everalbum consent order, prior settlements allowed companies, such as Google/YouTube and Facebook, to retain algorithms and technologies, including facial recognition technologies, that were created using wrongfully obtained data.

Chopra indicated that, in his view, it was important for the FTC to require a violator of data protection laws to "forfeit the fruits of its deception." Since both the Google/YouTube and Facebook settlements were approved during the Trump administration by 3-2 votes of the FTC commissioners, a likely shifting composition of the FTC under the Biden administration could bring a shift in the way that the FTC approaches AI/ML models of companies that have misused data.

Thus, companies should be particularly focused on ensuring that their policies and practices related to data collection and use are clear, particularly with respect to AI/ML models. And, where companies have used data in a manner inconsistent with or not clearly disclosed by their privacy policies, they should consider whether to prophylactically retrain such AI/ML models using "clean" data. Moreover, as Chopra has been nominated by President Joe Biden to lead the Consumer Financial Protection Bureau, financial services companies should be particularly attuned to these issues.

Also noteworthy is the Everalbum consent order's requirement to clearly and conspicuously disclose, separate from a privacy policy or similar document, Everalbum's intended use of biometric information. While not a general legal requirement, the FTC's imposition of this penalty may indicate that the FTC views such a consent as a best practice, consistent with “just-in-time” or “privacy notices in context,” which are considered best practice in a privacy-by-design approach. Accordingly, companies making use of biometric information should evaluate the policies and practices they currently use to seek consent to utilize biometric information and evaluate whether such policies and practices should be updated in light of privacy-by-design principles.

The knock-on effects from the Everalbum consent order also are worth considering. For instance, it is often the case that developers of AI/ML models use the data of their customers’ end-users to create such AI/ML models while also taking the stance that they are data processors/service providers, not data controllers/businesses, with respect to their use of the customers’ end-user data.

In light of the Everalbum consent order, such companies should carefully evaluate: (1) the privacy policies and end-user facing statements that their customers make and the consents that their customers’ end-users are required to give; (2) the data rights provisions in the agreements between the developer of the AI/ML models and its customers; (3) the data used to train the AI/ML models; (4) the uses to which the AI/ML models are put; and (5) whether, given the considerations in (1)-(4), the company training the AI/ML models and its customers truly have a processor/service provider relationship.

As these customer agreements are often heavily negotiated, and customers inevitably have varied privacy policies and practices, developers of AI/ML models should consider putting common contractual requirements in all customer agreements, requiring customers to provide certain disclosures and seek certain consents of end-users, and determining what limitations should apply to the developer's use of customer data where it is unable to impose such obligations. Further, developers of AI/ML models should have some right or mechanism to audit customers to ensure that the customers’ privacy policies and practices are consistent with their contractual obligations.

Many companies already use tools like data mapping to understand where data comes from, where it goes and how it is used; however, companies also should consider creating a data lineage for each of their AI/ML models to document what data sources were used to train such AI/ML models, together with any restrictions on use that may apply to the outputs of those AI/ML models. Such documentation can be used to help ensure that AI/ML models are only used in manners compliant with the restrictions on the use of the underlying data used to train them. And, if a company is challenged to prove the provenance of an AI/ML model, its data lineage will allow that company to demonstrate that the model was developed using appropriate data.

Takeaways

- The Everalbum consent order may indicate a shift in enforcement focus, as the FTC has indicated that it may require the deletion of AI/ML models developed based on data acquired without proper authorization. Given this potential shift, companies employing AI/ML models, particularly in the financial services industry, should make sure to scrutinize present and past uses of data to train AI/ML models to ensure that they will not be subject to an order requiring the deletion of the AI/ML models.
- Companies that use biometric and other sensitive personal information to train AI/ML models should reevaluate the use of privacy-by-design principles, including the timing and scope of disclosures made and consents sought from the providers of such biometric or other sensitive personal information.
- In addition to employing data mapping to track how data flows within an organization, companies should document the data lineage of their AI/ML models, together with any applicable restrictions on how those models can be used. This will help ensure compliance with data privacy laws and demonstrate clear ownership of AI/ML models.
- Customer agreements and the data-use provisions therein should be reviewed in light of the Everalbum consent order to ensure that developers of AI/ML models, and their customers, are in compliance with applicable data privacy laws.