Destruction Emerges as a Powerful Enforcement Measure for AI: FTC Requires Company to Delete Models Trained with Improperly Utilized Consumer Data

January 19, 2021

INTRODUCTION

For those following emerging artificial intelligence ("AI") regulations and enforcement closely, one issue of great interest is remedies. In particular: in what circumstances, if any, would regulators or courts find that a flawed machine learning or AI model must be scrapped entirely? A hot-off-the-press decision from the U.S. Federal Trade Commission (the "FTC") suggests regulators will not shy away from saying "scrap it."

The issue arises when a complex model is trained utilizing data that the model owner was not legally authorized to use for that purpose. Examples that might, in time, attract regulatory or judicial scrutiny include AI tools that:

- Identify fabricated news stories by reference to verified news articles from reputable sources, but in violation of copyright laws.
- Screen resumes and decide which job applicant gets to the interview stage of the process—with the tool trained using the resumes of poorly performing employees, without their knowledge or consent.
- Review loan applications and decide who is an unacceptable credit risk, based in part on data scraped from the Internet in violation of the terms of use of certain websites.

If it is determined that an AI model learned from training data that it was not supposed to utilize, two questions arise. ***First***, can the tainted data be removed from the model entirely, or does the nature of the model preclude that possibility? And ***second***, whether or not the model can be completely cleansed of the tainted data, what is the appropriate remedy—should the model owner pay a penalty or compensation for the misuse of the training data, should the person whose data was misused have some ownership interest in the model or should the model be mothballed?

On January 11, 2021, the FTC adopted the mothball approach, entering into a settlement requiring Everalbum, Inc. ("Everalbum"), a company that used AI for facial recognition, to "forfeit the fruits of its deception." Everalbum was obligated to delete any facial recognition models and algorithms it developed using photos or videos uploaded by its users without their consent—contrary to a promise from Everalbum to provide a consent opportunity. FTC Commissioner Rohit Chopra remarked in a statement that Commissioners have previously voted to allow data protection law violators to retain algorithms and technologies that derive much of their value from ill-gotten data and that the Everalbum settlement marked an "an important course correction."

This settlement may have significant implications for companies that rely on consumer data to train and operate AI applications—or that license AI from third parties—given the increased risk of losing valuable models and algorithms as the result of an enforcement action.

BACKGROUND

Everalbum offered a free app called "Ever" that allowed users to upload photos and videos from their mobile devices, computers or social media accounts to the cloud for storage and organization. In February 2017, Everalbum introduced a facial recognition feature called "Friends" that allowed users to "tag" people by name in their photos. Everalbum simultaneously used millions of facial images extracted from Ever users' photos along with publicly available facial images to create four datasets to further develop its facial recognition technology. It then sold the facial recognition technology to enterprise customers (though it did not directly share with the enterprise customers any Ever users' photos, videos or personal information).

According to the settlement, between July 2018 and April 2019, Everalbum represented to users that it would not apply facial recognition to users' content unless a user affirmatively opted in. But, in fact, facial recognition was automatically active for most of the company's users and could not be turned off. Everalbum allegedly also promised that user photos and videos would be deleted if a user de-activated their Ever account, but until at least October 2019, Everalbum failed to do so.

FIVE KEY TAKEAWAYS FOR CORPORATE AI AND ALGORITHMIC-BASED APPLICATIONS

Regulators Are Using Existing Legal Tools to Bring AI Enforcement Actions

As we have noted previously, the SEC, the FTC and other regulators are not waiting for new AI-specific regulations to bring enforcement actions related to the use of complex models. Here, the FTC alleged that Everalbum's misrepresentations regarding the use of its customers' photos for the purpose of developing and improving facial recognition AI models constituted unfair or deceptive acts or practices in violation of Section 5(a) of the Federal Trade Commission Act.

Notably, the FTC Act was passed in 1917, when AI was not exactly on anybody's mind, and it gives the FTC basically just two legal powers in the consumer protection space: to punish "unfair" and "deceptive" practices. But while various AI-specific proposals percolate in various legislatures, the FTC is not hesitating to use its century-old anti-deception power to punish modern-day tech practices.

Consider Ways to Reduce Risk of Misusing Data in AI Training

Although Everalbum involved facial recognition technology, the language of the settlement and accompanying statement suggests that the FTC's "course correction" may apply to AI applications more broadly. Companies investing heavily in AI should consider implementing policies, procedures and training designed to ensure that the company is fully authorized to use the AI training data for this purpose. Such companies should also take steps to make sure that there is sufficient documentation of such efforts.

The Increased Need for AI Diligence for Vendors and Acquisitions

Companies are increasingly bolstering their AI capabilities through acquisitions or third-party vendor arrangements. In light of this settlement, companies should consider implementing a robust AI diligence and risk-assessment process for third-party AI applications that could include:

- Determining whether the AI application was developed using sensitive consumer data—including biometric information or data concerning protected class membership—or other data that may be subject to claims of unauthorized use;
- Assessing what steps the vendor or acquisition target took to ensure that all the appropriate authorizations were obtained; and
- Evaluating the documentation associated with those authorizations.

Consider Ways to Mitigate Risks and Costs Related to Tainted Models

To the extent that a company has already collected and used data for training that may be viewed as problematic in some way, efforts should be made to determine whether any remediation is possible by:

- Providing appropriate after-the-fact notice of the data's use or obtaining necessary consents;
- Completely purging the potentially tainted data from the model, to the extent possible, and documenting that process, perhaps with the assistance of a third-party firm to provide some testing or audit of the process;
- Planning for any business disruption that would result if the company were obligated to temporarily or permanently cease to use the model;
- Ensuring that the risk that the model may have to be scrapped due to tainted training data is sufficiently disclosed to the board and investors; and
- Assessing whether the risks can be further mitigated with insurance or otherwise.

Stay Abreast of Potential Changes to the FTC's Monetary Penalty Authority and Enforcement Priorities

It is worth noting that the FTC's interest in a remedy that disabled the model in question was likely influenced by the fact that the FTC did not have civil penalty authority in this situation. Indeed, Commissioner Chopra's statement laments the FTC's inability to seek civil penalties against first-time offenders, given that it has not yet codified restrictions on the unlawful practices into a rule pursuant to Section 18 of the FTC Act.

Notably, the Everalbum settlement also comes at a time when the FTC's ability to seek consumer redress is also under question. The U.S. Supreme Court is poised this year to decide whether the FTC is entitled to recover monetary relief in civil enforcement actions under Section 13(b) of the FTC Act. While the Supreme Court initially granted petitions for certiorari on this issue in two cases from the Seventh and Ninth Circuits (which reached opposite conclusions), it has since vacated its grant in the former case, leaving only the Ninth Circuit case before the Court. Oral arguments recently took place on January 13, with a number of Justices suggesting that there is no evidence based upon the statutory text that Congress intended to grant the FTC the power to obtain monetary remedies in cases brought under Section 13(b).

If the Supreme Court rules against the FTC, it is possible that legislation would be introduced in the near future that would, if enacted, expressly grant the FTC the authority to obtain monetary remedies under Section 13(b). Commissioner Chopra has also separately advocated for the FTC to use additional tools—including its largely abandoned Penalty Offense Authority under Section 5(m)(1)(b) of the FTC Act—to more forcefully deter harmful conduct by seeking civil penalties for first-time offenses.

Companies should stay abreast of developments concerning the FTC's ability to seek restitution and monetary penalties, as well as the potential for increased scrutiny of AI by the incoming Biden Administration. We will continue to update you on further developments in this area.

To subscribe to the Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Justin C. Ferrone
jcferrone@debevoise.com

Anna R. Gressel
argressel@debevoise.com

WASHINGTON, D.C.

Paul D. Rubin
pdrubin@debevoise.com

Melissa Runsten
mrunsten@debevoise.com