Legal Considerations When Using Consumer Data To Train AI

By **James Gatto** (June 22, 2023)

James Gatto

Many companies are sitting on a trove of customer data and are realizing this data can be valuable to train artificial intelligence models.

However, what some companies have not thought through, is whether they can actually use that data for this purpose. Sometimes this data is collected over many years, often long before a company thought to use it for training AI.

The potential problem is that the privacy policies in effect when the data was collected may not have considered or disclosed this use.

Using customer data in a manner that exceeds or otherwise is not permitted by the privacy policy in effect at the time the data was collected could be problematic. This has led to class actions and enforcement by the Federal Trade Commission.

In some cases, the FTC has imposed a penalty known as algorithmic disgorgement to companies that use data to train AI models without proper authorization. This penalty is severe as it requires deletion of the data, the models and the algorithms built with it — and can be an incredibly costly result.

For example, the FTC filed an administrative complaint against Everalbum Inc. in January 2021. Everalbum provided a photo album and storage application but used the customers' photos and videos for other purposes.

Everalbum created new datasets, often without user permission, that it used to train its facial recognition technology to create a different application. It also did not delete photos and videos from users who deactivated their accounts.

The FTC settled with Everalbum for AI and privacy violations, with the result being that Everalbum had to destroy various data, algorithms and models.

This is an example of algorithmic disgorgement. It requires a party to destroy ill-gotten or improperly used data, along with the models and algorithms built with it. Some have analogized this to the concept of the fruit of the poisonous tree.

The scope of algorithmic disgorgement can be broad. It has been defined comprehensively by the FTC to include any models or algorithms developed in whole or in part using data or other content that was improperly collected or used.

It is important to note that this definition can cover data that was either improperly collected or data that was properly collected but used for a purpose beyond that which was disclosed to or agreed to by the users from whom the data was collected. This is clear from the fact that even the FTC acknowledged that Everalbum did not improperly obtain the photos and videos.

The photos and videos were voluntarily uploaded by users for storage and to generate albums and Everalbum properly obtained consent for that purpose. The problem was that it used that content to train AI models without consent and retaining that content after ensuring users it would be deleted upon account deactivation.

Another important component of the FTC settlement with Everalbum was the nature of the disclosure required to use collected data to train AI models.

The settlement required Everalbum, before using any data to train, develop, or alter any face recognition model or algorithm, to clearly and conspicuously disclose to the user from whom it has collected the data, separate and apart from any "privacy policy," "terms of use" page, or other similar document, all purposes for which Everalbum will use, and to the extent applicable, share, the data and obtain the affirmative express consent of the user from whom it collected the data.

It is not clear from this alone that a separate disclosure of such use is always required, but it may be safer to do so. Thus, it may be beneficial to consider including such disclosure in the privacy, but also include a separate pop-up disclosure to which a user must affirmatively consent.

In another algorithmic disgorgement case, the FTC in 2019 settled with a data analytics and consulting company engaged in the practice of deceptively harvesting personal information from social media sites and required the deletion of the information and any algorithms or equations, that originated, in whole or in part, from this information.

In March 2022, the FTC settled with a weight loss app used by children, WW International Inc. — formerly known as Weight Watchers — and its subsidiary, Kurbo by WW, and required deletion of data and models and/or algorithms developed in whole or in part while using the personal information collected from the children.

While these FTC actions are worth heeding, the FTC is not the only threat to companies training AI models. Class action attorneys are circling the waters and smell blood.

At least one recent class action has been filed based on the use of images uploaded by users to train AI models, arguably without the proper consent to do so.

In Flora v. Prisma Labs Inc. filed in February in the U.S. District Court for the Northern District of California, the plaintiffs allege that Prisma's app, Lensa, allows users to upload their selfies for editing and retouching and that Prisma:

- Collects the photo subject's biometric data, facial geometry, in a nonanonymized fashion;
- Offers a confusing and false disclosure of its collection practices;
- Retains the subject's biometric data in a nonanonymized fashion;
- Retains that data indefinitely for uses wholly unrelated to the user's purpose for using Lensa;
- Profits from the biometrics; and
- Has no public written policy for the deletion of that data.

Allegedly, the privacy policy fails to disclose the use of the biometric data and other information Prisma collects from its users and from the images uploaded through app in violation of the Illinois Biometric Information Privacy Act.

The plaintiffs are seeking money damages and equitable, injunctive and declaratory relief.

While the complaint does not specifically request algorithmic disgorgement, it is not clear whether the court will issue an order imposing algorithmic disgorgement should the plaintiffs prevail.

The foregoing cases primarily address situations where companies used data they already had to train AI models, at least arguably without consent to do so. Many companies are newly collecting data and content from various sources to build databases upon which they can train AI models.

In these cases, it is important to ensure that data is properly acquired and that its use to train models is permitted. This too has led to lawsuits and more will likely be filed.

The issues in cases of newly collected data are somewhat fact dependent. They depend on the type of data, how it is collected and from where it is collected.

For example, sometimes the content is copyright protected — e.g., images — and can constitute infringement.

In two suits against Stability AI Inc. — one in the U.S. District Court for the Northern District of California and the other in the U.S. District Court for the District of Delaware, both filed in January — the plaintiffs have alleged that the method used to train models on their images constitutes copyright infringement and the defendant has alleged it is not infringement, or it is fair use under U.S. copyright law.

Fair use is a concept under U.S. copyright law but does not apply in many other jurisdictions. This has led some companies that train AI models to forum shop for a legally favorable venue to do so.

For example, Japan has recently declared that using datasets for training AI models doesn't violate copyright law. This decision presumptively means that model trainers can gather publicly available data without having to license or secure permission from the data owners.

Another type of content used to train AI models — e.g., for AI-based code generators — is source code. Typically, the code is obtained from open source repositories under an open source license.

These licenses typically permit use of the code for any purpose subject to certain license conditions — e.g., giving attribution, maintaining copyright notice or providing the license terms.

Because broad use is permitted, training AI models likely is not infringement. But failure to comply with the conditions can breach the license.

This scenario is at issue in Doe 1 v. GitHub Inc. filed in the U.S. District Court for the Northern District of California in November 2022, where the AI models are trained on code available under open source licenses.

This case does not allege infringement, but rather violations of the Digital Millennium Copyright Act because the outputs do not include the copyright management information, and breach of the open source license for failing to comply with conditions in the open source licenses.

Some AI code generators have tools to manage open source compliance issues. Various other tools exist and are being developed to help mitigate legal risk with generative AI.

For some generative AI applications, there are different versions for individual use and enterprise use. Many companies that use generative AI and develop policies for such use mandate that employees use the enterprise version that includes these tools.

Another category of content used to train AI models includes images licensed under a Creative Commons or similar licenses. The perception by many is these licenses are like open source licenses and broadly permit any use.

Many people fail to realize there are six different versions of the license. Three of these prohibit commercial use, two prohibit any making any derivatives, and all require attribution.

Thus, it is important to understand which version of the Creative Commons license applies to any content for which you want to use to train AI and that you consider any restrictions — no commercial use, no derivatives — and compliance obligations, such as attribution.

Conclusion

The rapid growth of generative AI has led to a flurry of activity, including the training of AI models on various types of content.

Whether you are training models based on content you already possess or are newly acquiring, it is important to ensure you have the right to use that content for those intended purposes. This includes clearly disclosing and obtaining consent to such use.

The issues in each situation are fact dependent, including the nature of the content, how it was obtained, any agreements or policies relevant to such use, and for what the AI tool is used.

Sometimes, for example, with AI-based medical tools, other regulatory issues may be relevant. Training AI models for use in other regulated industries or uses may implicate other considerations.

Training AI models is just one area in which legal landmines can arise in connection with generative AI. Various issues arise with training AI, user inputs and the outputs.

Companies entering this space or using these tools would be well served to develop a policy on employee use of generative AI.

James Gatto is a partner, co-leader of the blockchain and fintech team, and leader of the open source team at Sheppard Mullin Richter & Hampton LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.