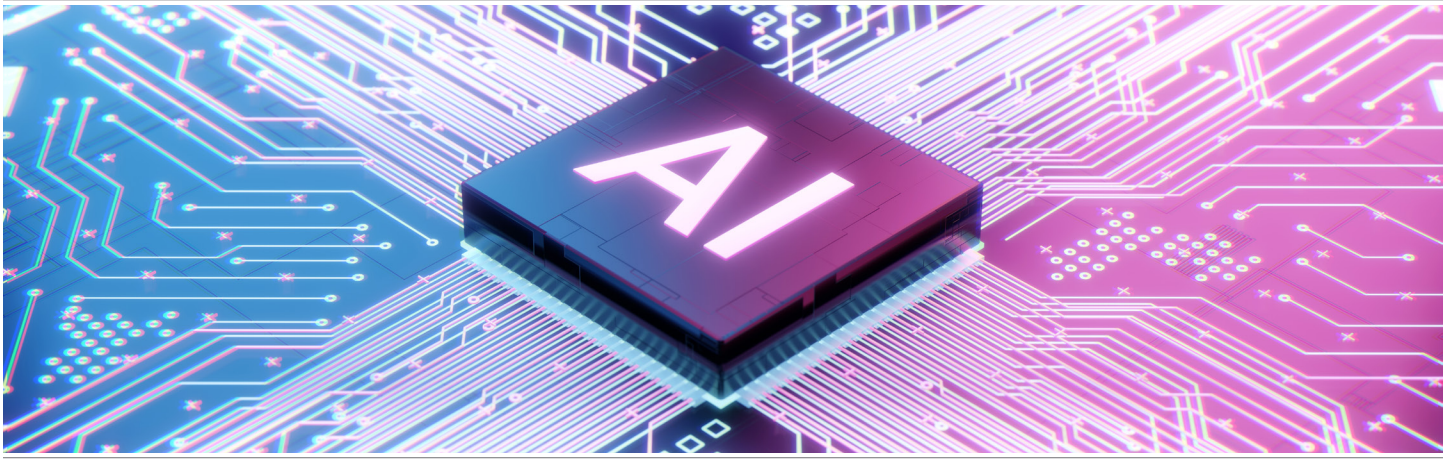
SheppardMullin



Training AI Models – Just Because It's "Your" Data Doesn't Mean You Can Use It

By: James Gatto and Moriah Dworkin

Many companies are sitting on a trove of customer data and are realizing that this data can be valuable to train AI 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 this use. The use of 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 action lawsuits and/or enforcement by the FTC. 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. This can be an incredibly costly result.

The following are examples of cases where a company utilized customer data to train AI models/algorithms and their right to do so was questioned.

In January 2021, the FTC filed an administrative complaint against Everalbum, Inc. ("Complaint"). Everalbum created a photo and video storage application named "Ever," which allowed consumers to upload digital photos and videos to Ever's cloud servers. Ever used automated features to organize users' digital photos and videos into albums by location and date. In May 2021, the FTC settled with Everalbum for AI/privacy violations by requiring them to **destroy various data, algorithms, and models**.

Everalbum subsequently extracted millions of facial images from users' photos it obtained from publicly available sources, in order to create new datasets it used to train its facial recognition technology. Everalbum used that facial recognition technology in its Ever app to provide services to enterprise customers for purposes such as security, access control, and facilitating payments. It did not share users' actual images with the enterprise customers.

The Complaint alleged that Everalbum falsely represented that it was not using the facial recognition on consumer's photos unless the consumer affirmatively chose to activate that feature. Rather, it automatically activated its face recognition feature—which could not be turned off—for all mobile app users, except those who lived in three U.S. states and the European Union. The Complaint also alleged that Everalbum failed to keep its promise to delete the photos and videos of the Ever users who deactivated their accounts, and instead retained them indefinitely.

As part of the settlement with the FTC, Everalbum was forced to delete the photos and videos of all the Ever app users who deactivated their accounts, along with the models and algorithms it developed by using the photos and videos uploaded by its users.

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. This is a significant penalty as training AI models can cost tens or hundreds of millions of dollars. Destroying the models wipes out this investment.

As part of these proceedings, the FTC issued a Decision and Order ('Order") which set forth the scope of the algorithmic disgorgement. The following are some details of that Order.

First, the FTC defined some of the key terms. Among the definitions are:

- "Affected Work Product" is defined as any models or algorithms developed in whole or in part using Biometric Information Respondent collected from Users of the "Ever" mobile application.
- "Biometric Information" is defined as data that depicts or describes the physical or biological traits of an identified or identifiable person, including depictions (including images), descriptions, recordings, or copies of an individual's facial or other physical features (e.g., iris/retina scans), finger or handprints, voice, genetics, or characteristic movements or gestures (e.g., gait or typing pattern).
- "Covered Information" is defined as information from or about an individual consumer, including (10) Biometric Information; (11) descriptive information derived from Biometric Information, including a Face Embedding…
- "Face Embedding" is defined as data, such as a numeric vector, derived in whole or in part from an image of an individual's face.

The Order then set forth several requirements, including:

- A prohibition against various misrepresentations relating to Covered Information;
- Prior to using Biometric Information collected from a User to (1) create a Face Embedding or (2) train, develop, or alter any face recognition model or algorithm, clearly and conspicuously *disclose* to the User from whom Respondent has collected the Biometric Information, *separate and apart from any "privacy policy," "terms of use" page, or other similar document*, all purposes for which Respondent will use, and to the extent applicable, share, the Biometric Information; and obtain the affirmative express consent of the User from whom Respondent collected the Biometric Information; and
- *Delete or destroy all photos and videos* that Respondent collected from Users who requested deactivation of their Ever accounts by the issuance date of this Order, and provide a written statement to the Commission, sworn under penalty of perjury, confirming that all such information has been deleted or destroyed; *delete or destroy all Face Embeddings* derived from Biometric Information Respondent collected from Users who have not, by that date, provided express affirmative consent for the creation of the Face Embeddings, and provide a *written statement* to the Commission, sworn under penalty of perjury, confirming that all such information has been deleted or destroyed; and *delete or destroy any Affected Work Product*, *and* provide a written statement to the Commission, sworn under penalty of perjury, confirming such deletion or destruction.[1]

[1] A copy of the compliance report is here. Note, the report was submitted by Paravision, Inc. After the Order was issued against Everalbum, Inc., it decided to start do business as Paravision, Inc.

A few points to note based on the Everalbum settlement and Order:

First, Everalbum did not improperly obtain the photos and videos. They were uploaded by users for storage and to generate albums, so Everalbum properly obtained that content. The problem was the manner in which it used that content once Everalbum obtained it. Specifically, using the content to train AI models without consent and retaining that content after ensuring users it would be deleted.

This leads to a key takeaway which is that although you properly obtained data or content, this alone does not necessarily mean you can use it to train AI models and you must ensure that you are accurately representing the scope of how you are using data or content to users.

Second, the scope of the Affected Work Product under the algorithmic disgorgement was quite broad. It included *any* models or algorithms developed *in whole or in part* using Biometric Information Respondent collected from Users of the "Ever" mobile application. This is pretty comprehensive.

Third, the Order did not permit Everalbum to just include the disclosure of use in a "privacy policy," "terms of use" or other similar document. It is not clear from this alone that a separate disclosure is always required, but sometimes it may be safer to do so.

This is not the only case where algorithmic disgorgement has been applied. In 2019, the FTC settled with a data analytics and consulting company engaged in the deceptive practice of harvesting personal information from social media sites. The Order required the company to delete and/or destroy all "Covered Information" collected from consumers and any information or work product, including all algorithms or equations it originated, in whole or in part, from this Covered Information. In March 2022, it settled with a weight loss app used by children. That Order required deletion of data and models and/or algorithms developed in whole or in part while using the personal information collected from children.

The rise of generative AI has inspired many companies to leverage the data and content they have amassed over the years, to train AI models. It is important that these companies ensure they have the right to use this data and content for this purpose. The lessons from Everalbum 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 suit 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 et al v. Prisma Labs, Inc.* (February 2023) the complaint alleges that Prisma develops mobile apps, including "Lensa," to allow users to upload their "selfies" for editing and retouching. It later added a "magic avatar" feature that requires a user to upload 8 to 20 selfies, which it then processes to generate a "magic avatar."[2] When creating a "magic avatar," Prisma collects facial geometry associated with the uploaded images. It then uses that facial geometry not only to create the "magic avatar," but to also train its neural network algorithms. The complaint further alleges that every time the app is opened, the user is given two options: "Add photos" or "Magic Avatars." Regardless of which

[2] The complaint makes other allegations that will not be addressed in detail herein. These allegations include that a user can create an avatar for anyone by uploading a collection of the non-user's images. Avatars of celebrities (not created by the celebrities themselves) have already circulated widely on social media and there is nothing to stop a user from providing images of an ex-spouse/partner, school rival, unfriendly neighbor, or family member, even for insidious purposes. This possibility is particularly worrisome given the fact that the Lensa app often generates highly sexualized images, particularly of women.

option is chosen, the user cannot proceed without first giving Lensa access to all photos stored on their device.[3]

The complaint further alleges that Prisma: (1) collects the photo subject's biometric data (facial geometry) in an non-anonymized fashion; (2) offers a confusing and false disclosure of its collection practices; (3) retains the subject's biometric data in a non-anonymized fashion; (4) retains that data indefinitely for uses wholly unrelated to the user's purpose for using Lensa; (5) profits from the biometrics; and (6) has no public written policy for the deletion of that data.

Allegedly, the Lensa 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 Lensa.[4]

The complaint alleges various causes of action, including:

- Violation of Illinois Biometric Information Privacy Act, 740 ILCS 14/15(a) which requires that a "private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first."
- Violation of Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b)(1) which provides, "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first … informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored."
- Violation of Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b)(2) which provides, "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first … informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used."
- Violation of Illinois Biometric Information Privacy Act, 740 ILCS 14/15(b)(3) which provides "No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first … receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."
- Violation of Illinois Biometric Information Privacy Act, 740 ILCS 14/15(c) which provides, "No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information."
- Violation of Illinois Biometric Information Privacy Act, 740 ILCS 14/15(d) which provides, "No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information" absent disclosure of such practice and the customer's consent."

---

[3] The complaint also alleges that while creating the avatars, the app uses Stable Diffusion, an open-source AI model which was originally trained on 2.3 billion captioned images from various third-party sites from the internet. The provider of this tool has been sued for alleged infringement.

[4] The complaint alleges many other facts but the foregoing provides an idea of the issues.

- Violation of Illinois Biometric Information Privacy Act, 740 ILCS 14/15(e) which provides, "A private entity in possession of a biometric identifier or biometric information shall (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."

Given this is a class action suit, the plaintiffs are primarily seeking money damages but they also seek "equitable, injunctive and declaratory relief." The complaint does not specifically request algorithmic disgorgement as part of this relief. If the plaintiffs prevail, it is not clear whether the court will issue an order imposing algorithmic disgorgement. This case remains pending and we plan to monitor this one.

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. Sometimes, plaintiffs allege that the companies have collected and used content that is copyright protected.[5] These cases include allegations that the method used to train models constitutes infringement. In defense, the companies argue, in part, this is a fair use under U.S. copyright law.

In another case *Doe 1 et al v. GitHub, Inc. et al*, a class action suit involving AI code generators, the AI models are trained on source code available under open source licenses. This case does not allege infringement, presumably because the open source licenses grant broad rights to use for any purpose. Rather, this case includes allegations that such use violates the Digital Millennium Copyright Act (DMCA) and breaches the open source license terms. These claims are based on the allegations that the outputs of these code generators remove copyright management information in violation of the DMCA and fail to comply with conditions in the open source licenses (e.g., giving attribution, maintaining the copyright notice and/or providing the License Terms) thus breaching the licenses.

For more information on legal issues with AI code generators and how you can mitigate legal issues when using them, see Solving Open Source Problems with AI Code Generators – Legal Issues and Solutions.

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.

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, with AI-based medical tools, other regulatory issues may be relevant. For example, see ChatGPT And Healthcare Privacy Risks. Another example is, if you are dealing with the government, other considerations may also be relevant. See ChatUSG: What government contractors need to know about AI. Training AI models for use in other regulated industries or uses may implicate other considerations.

[5] These include suits against Stability AI including one filed by an online image service and another by a group of artists. These cases remain pending as of the time of writing.

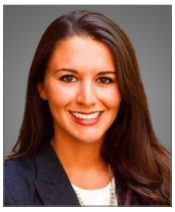
Training AI models is only one area in which legal landmines can arise in connection with use of generative AI. Companies entering this space or using these tools would be well served to develop a policy on employee use of generative AI. For examples of what these policies should include and why you need them, see AI Technology – Governance and Risk Management: Why Your Employee Policies and Third-Party Contracts Should be Updated.

As companies enter the generative AI space, in-house counsels are scrambling to get up to speed on these issues and develop policies to mitigate the associated legal risk. Many companies have found it helpful to have knowledgeable counsel conduct an in-house presentation on legal issues with generative AI to assist in understanding the growing number of legal issues and how to develop company-specific policies.

If you have questions on these issues, contact us to discuss.

For further details, please contact:

James Gatto
Member, SheppardAI
bio
202.747.1945
jgatto@sheppardmullin.com



Moriah Dworkin
Associate
bio
310.228.2297
mdworkin@sheppardmullin.com

Sheppard Mullin is at the forefront of legal issues with Artificial Intelligence (AI), including the rapidly growing use of generative AI. Several of our attorneys, including those in our Intellectual Property and Technology groups, have technical backgrounds that enable us to understand the technical workings of AI tools and the component technologies that comprise AI. Our team includes attorneys with diverse legal backgrounds who collectively understand the vast array of legal issues with and ramifications of AI technology, with some advising clients on AI issues for nearly two decades. In addition to advising clients on a wide variety of legal issues related to AI, our team routinely helps companies develop policies on employee use of generative AI and has conducted many in-house training seminars on these issues.