Legal Issues When Training AI On Previously Collected Data

By **James Gatto** (March 20, 2024)

James Gatto

Many companies are sitting on a trove of customer data and realizing that this data can be valuable to train AI models. What some companies have not thought through is whether they can properly 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. However, 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.[1]

As companies think through these issues and consider how to overcome this problem, some have, or will, update their terms of service or privacy policy to address this. Before companies make such changes, it is critical to ensure any such change is legally effective. Proper notice and consent are prudent.

Companies considering changes to their terms of service or privacy policy should be aware of recent guidance from the Federal Trade Commission. On Feb. 13, the FTC issued guidance titled "AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive."[2] In this guidance, the FTC warned:

It may be unfair or deceptive for a company to adopt more permissive data practices — for example, to start sharing consumers' data with third parties or using that data for AI training — and to only inform consumers of this change through a surreptitious, retroactive amendment to its terms of service or privacy policy.

The FTC further warned that market participants should be on notice that any firm that reneges on its user privacy commitments risks running afoul of the law. Simply put, according to the guidance, a business that collects user data based on one set of privacy commitments cannot then unilaterally renege on those commitments after collecting users' data.

The guidance gave two examples where the FTC challenged what it believed to be deceptive and unfair practices in connection to each company's privacy policy that affected the promises the company previously made to consumers.[3]

In one example, the FTC in 2004 undertook a successful enforcement action against Gateway Learning Corp., which rented to third parties customer information it had pledged to keep private. Gateway later tried to change its privacy policy without notifying consumers, who had already provided their information, to say that it had revised its privacy policy. Gateway also did not highlight on its website that its privacy policy had changed.

The guidance also referenced the FTC's enforcement action last summer against 1Health.io, which deceived consumers about their ability to get their data deleted, and changed its privacy policy retroactively without adequately notifying and obtaining consent from consumers whose data the company had already collected.

These two cases were not specifically related to using customer data to train AI models. However, the FTC has addressed the use of customer data to train AI models in other cases.

One of the ramifications of improperly using customer data to train AI models is a severe remedy referred to as algorithmic disgorgement, which requires deletion of the data, the models and the algorithms built with it. This can be an incredibly costly result due to the high cost of training AI models.

One example of algorithmic disgorgement was a settlement reached by the FTC in January 2021 with Everalbum Inc. In that matter, the FTC filed an administrative complaint against Everalbum, which created a photo and video storage application called Ever. This application 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.

Everalbum later extracted millions of facial images from users' photos to create new datasets it used to train its facial recognition technology. A key aspect of 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. 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.

In May 2021, the FTC settled with Everalbum for AI and privacy violations and sought algorithmic disgorgement, requiring Everalbum to destroy its data, algorithms and models.

In the guidance, the FTC further warned that it will continue to bring actions against companies that engage in unfair or deceptive practices — including those that try to switch up the "rules of the game" on consumers by surreptitiously rewriting their privacy policies or terms of service without proper notice to, and consent by, customers, to allow themselves free rein to use consumer data for product development.

A key takeaway is that companies need to carefully think through their terms of service and privacy policies and be cautious when changing them to permit new uses of previously collected data.

Managing the use of data of any type for training AI can implicate several legal considerations. To obtain a sense of the scope of the issues on which the FTC is focused, it is instructive to consider the 20-page civil investigative demand letter the FTC sent to OpenAI.[4] The letter probes in detail for documents, facts and policies relating to all facets of OpenAI's business including:

- Its training, testing, refining, marketing and managing of its large language models, or LLMs, including identification of the data used to train the models, how the data was obtained, and the sources of the data;
- Policies for assessing and addressing risks, and ensuring the safety and accuracy of the LLMs;
- Steps it takes to avoid infringement or privacy violations by the LLMs;
- Details of its monitoring, collecting, using, retaining and deleting personal data of users interacting with the LLMs; and

- Many other topics.

The topics addressed in the civil investigative demand letter comprise a good checklist of issues to be considered by companies developing AI models.

Companies that train AI models are strongly recommended to develop policies to address the myriad legal issues that can arise. Companies that develop AI technology should adopt policies and procedures to ensure responsible use of AI and mitigate any liabilities. A small sample of the things that companies should address includes:

- Developing policies and procedures on the collection and use of data to train the AI models to ensure the right to use that data;
- Assessing risk and safety issues before releasing a new model or product based thereon;
- Ensuring the models do not result in biased or discriminatory outputs; and
- Preventing personal information from improperly being used in the training data or outputting personal information or false or disparaging information about a person.

James Gatto is a partner at Sheppard Mullin Richter & Hampton LLP. He is co-leader of the firm's artificial intelligence team, the blockchain and fintech team, and leader of its open source team.

[1] See Training AI Models — Just Because It's "Your" Data Doesn't Mean You Can Use It.

[2] See AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive.

[3] See, e.g., Gateway Learning Corp. and 1Health.io.

[4] For an overview of some of the legal issues to consider, see The Need for Generative AI Development Policies and the FTC's Investigative Demand to OpenAI.