



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Technology Blog

AI Companies: Uphold Your Privacy and Confidentiality Commitments

By: Staff in the Office of Technology

January 9, 2024



Data is at the heart of AI development. Developing AI models can be a resource intensive process, requiring large amounts of data and compute,^[1] and not all companies have the capacity to develop their own models. Some companies, which we refer to as “model-as-a-service” companies in this post, develop and host models to make available to third parties via an end-user interface or an application programming interface (API). For example, a company can train a large language model (LLM) and sell access to this model to businesses (online stores, hotels, banks, etc.) who apply it to customer service chatbots.

Like most AI companies, model-as-a-service companies have a continuous appetite for data to develop new or customer specific models or refine existing ones. This business incentive to constantly ingest additional data can be at odds with a company's obligations to protect users' data,^[2] undermining peoples' privacy^[3] or resulting in the appropriation of a firm's competitively significant data. This risk is particularly salient given that customers may reveal sensitive or confidential information when using a company's models, such as internal documents and even their own users' data.^[4] There's also a risk that a model-as-a-service company may, through its APIs, infer a range of business data from the companies using its models, such as their scale and precise growth trajectories.

Model-as-a-service companies that fail to abide by their privacy commitments to their users and customers, may be liable under the laws enforced by the FTC. This includes promises made by companies that they won't use customer data for secret purposes, such as to train or update their models—be it directly or through workarounds. In its prior enforcement actions, the FTC has required businesses that unlawfully obtain consumer data to delete any products—including models and algorithms^[5] developed in whole or in part using that unlawfully obtained data. The FTC will continue

to ensure that firms are not reaping business benefits from violating the law.

Model-as-a-service companies must also abide by their commitments to customers regardless of how or where the commitment was made.^[6] This includes, for instance, commitments made through promotional materials, terms of service on the company's website, or online marketplaces. Failure to do so can expose a firm to enforcement action by the FTC. For example, the FTC has brought actions against companies that disclosed people's data for ad targeting despite assuring them in privacy policies^[7] or during the registration process^[8] that it would keep their data private. And if companies choose to retain or use consumer data for other purposes^[9] without providing clear and conspicuous notice and obtaining affirmative express consent^[10]—for example, by surreptitiously changing its terms of service or privacy policy,^[11] or burying a disclosure behind hyperlinks, in legalese, or in fine print^[12]—they risk running afoul of the law.

Additionally, what a company *fails* to disclose to customers may be just as significant as what it promises. The FTC can and does bring actions against companies that omit material facts that would affect whether customers buy a particular product—for example, how a company collects and uses data from customers. The FTC brought an action^[13] against a company that, among other things, claimed not to use its facial recognition technology on consumers' images unless consumers affirmatively chose to activate the feature—but omitted the fact that this was only true for consumers in *some* jurisdictions. This omission subjected the company to the same type of enforcement as if it had made an explicit misrepresentation.

Misrepresentations, material omissions, and misuse of data associated with the training and deployment of AI models also pose potential risks to competition. These tactics can undermine fair competition by, among other things, luring and locking in customers based on false promises or allowing dishonest businesses to get a leg up over honest businesses. Model-as-a-service companies that appropriate the competitively significant information of business customers may also run afoul of the prohibition against unfair methods of competition. In short, the data practices of model-as-a-service companies can violate antitrust laws as well as consumer protection laws.^[14]

There is no AI exemption from the laws on the books. Like all firms, model-as-a-service companies that deceive customers or users about how their data is collected—whether explicitly or implicitly, by inclusion or by omission—may be violating the law.

Thank you to staff from across the Office of Technology, the Bureau of Competition, and the Bureau of Consumer Protection who collaborated on this post (in alphabetical order): Krisha Cerilli, Jessica Colnago, Julia Horwitz, Amritha Jayanti, Stephanie T. Nguyen. 

[1] Emily M. Bender, Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. 2021. On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? In Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT '21). Association for Computing Machinery, New York, NY, USA, 610–623. <https://doi.org/10.1145/3442188.3445922>

[2] For instance, users have concerns that companies will disclose user data to each other, (*see, e.g.*, <https://simonwillison.net/2023/Dec/14/ai-trust-crisis/>); and they may have concerns that models have leaked users' personal data to the public. *See, e.g.*, <https://www.computerworld.com/article/3711467/questions-raised-as-amazon-q-reportedly-starts-to-hallucinate-and-leak-confidential-data.html>; <https://www.fastcompany.com/90958811/google-was-accidentally-leaking-its-bard-ai-chats-into-public-search-results>; <https://www.pcmag.com/news/openai-confirms-leak-of-chatgpt-conversation-histories>

[3] This includes consumers, small businesses, and enterprise users.

[4] Similarly, a model-as-a-service company that makes its service available to end-users may get access to people's personal information, including health and financial data.

[5] <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>

[6] <https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check>

[7] <https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising>

[8] <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising>

[9] <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users>

[10] <https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc>

[11] <https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-finalizes-order-1healthio-over-charges-it-failed-protect-privacy-security-dna-data-unfairly>

[12] <https://www.ftc.gov/business-guidance/blog/2014/09/full-disclosure>



[13] <https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology>

[14] https://www.ftc.gov/system/files/ftc_gov/pdf/p241200_ftc_comment_to_copyright_office.pdf ; https://www.ftc.gov/system/files/ftc_gov/pdf/P221202Section5PolicyStatement.pdf .

Tags: [Technology](#) | [Artificial Intelligence](#) | [Office of Technology](#)

More from the Technology Blog

Technology Blog

The FTC Is on the Front Lines of Tech Innovation & Regulation

Stephanie T. Nguyen, Chief Technologist | January 17, 2025

Technology Blog

Behind the FTC’s 6(b) Report on Large AI Partnerships & Investments

Office of Technology Staff | January 17, 2025

Technology Blog

Surveillance Pricing Update & The Work Ahead

Stephanie T. Nguyen & Samuel A.A. Levine | January 17, 2025

Technology Blog

Lenses of security: Preventing and mitigating digital security risks through data management, software development, and product design for humans

Staff in the Office of Technology & the Division of Privacy and Identity Protection | December 13, 2024

Get Business Blog updates

Enter email address

Subscribe

