Federated learning is a way to train AI models without anyone seeing or touching your data, offering a way to unlock information to feed new AI applications.



the AI and data platform built for business.

Federated learning is a way to train AI models without anyone seeing or touching your data, offering a way to unlock information to feed new AI applications.

The spam filters, chatbots, and recommendation tools that have made artificial intelligence a fixture of modern life got there on data — mountains of training examples scraped from the web, or contributed by consumers in exchange for free email, music, and other perks.

Many of these AI applications were trained on data gathered and crunched in one place. But today’s AI is shifting toward a decentralized approach. New AI models are being trained collaboratively on the edge, on data that never leave your mobile phone, laptop, or private server.

This new form of AI training is called federated learning, and it’s becoming the standard for meeting a raft of new regulations for handling and storing private data. By processing data at their source, federated learning also offers a way to tap the raw data streaming from sensors on satellites, bridges, machines, and a growing number of smart devices at home and on our bodies.

Under federated learning, multiple people remotely share their data to collaboratively train a single deep learning model, improving on it iteratively, like a team presentation or report. Each party downloads the model from a datacenter in the cloud, usually a pre-trained [foundation model](https://research.ibm.com/blog/what-are-foundation-models). They train it on their private data, then summarize and encrypt the model’s new configuration. The model updates are sent back to the cloud, decrypted, averaged, and integrated into the centralized model. Iteration after iteration, the collaborative training continues until the model is fully trained.

This distributed, decentralized training process comes in three flavors. In horizontal federated learning, the central model is trained on similar datasets. In vertical federated learning, the data are complementary; movie and book reviews, for example, are combined to predict someone’s music preferences. Finally, in federated transfer learning, a pre-trained foundation model designed to perform one task, like detecting cars, is trained on another dataset to do something else, like identify cats. Baracaldo and her colleagues are currently working to incorporate foundation models into federated learning. Under one potential application, banks could train an AI model to detect fraud, then repurpose itl for other use cases.