Is federated learning (FL) safe?

- If an ML model is useful, it must reveal information about the data on which it was trained [1].

References

1. Melis et al. Exploiting unintended feature leakage in collaborative learning. In *IEEE Symposium on Security & Privacy*, 2019.