Reference (Privacy Leakage)

1. Hitaj, Ateniese, & Perez-Cruz. Deep models under the GAN: information leakage from collaborative deep learning. In *ACM SIGSAC Conference on Computer and Communications Security*, 2017.
2. Melis, Song, Cristofaro, & Shmatikov. Exploiting unintended feature leakage in collaborative learning. In *IEEE Symposium on Security & Privacy*, 2019.
3. Zhu, Liu, & Han. Deep leakage from gradients. In *NIPS*, 2019.
4. Orekondy, Oh, Zhang, Schiele, & Fritz. Gradient-Leaks: Understanding and controlling deanonymization in federated learning. *arXiv*, 2018.
5. Ateniese, Felici, Mancini, Spognardi, Villani, & Vitali. Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers. *International Journal of Security and Networks*, 2015.
6. Fredrikson, Jha, & Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In *CCS*, 2015.
7. Ganju, Wang, Yang, Gunter, & Borisov. Property Inference Attacks on Fully Connected Neural Networks using Permutation Invariant Representations. In *CCS*, 2018.
8. Jia, Salem, Backes, Zhang, & Gong. Property inference attacks on fully connected neural networks using permutation invariant representations. In *CCS*, 2019.