Investigations:

- Utility-Privacy Tradeoff
- Influence of Dataset Structure
  - Class Size
  - Number of Classes
  - Dataset Imbalance
- Influence of Data
  - Information Density
  - Colored Images
  - Class Similarity

Datasets

- MNIST
- FMNIST
- SVHN
- CIFAR-10
- CIFAR-100
- EMNIST

Dataset Modifications

- Class Size
- Number of Classes
- Dataset Imbalance

Data Measurements

- Entropy
- Compression Ratios
- Standard Deviation
- Fisher's Discriminant Ratio

Non-Private Model

$\varepsilon = \infty$

Private Model

$\varepsilon = 30$

Private Model

$\varepsilon = 1$

- Accuracy
- F1-Score
- Train-/ Test Accuracy Gap

Utility Measurement

Vulnerability Measurement

- LiRA Attack
- AUC
- TPR @ FPR=0.1
- TPR @ FPR=0.001