Differentially Private SGD on Tabular Data: An Empirical Study on Adult Income

Shaurya Singh
University of Waterloo
Email: shaurya.singh12006@gmail.com | GitHub: Link

---

1. Motivation

Differential Privacy (DP) provides formal guarantees against leakage of individual training examples, but is often perceived as significantly degrading model utility. While many theoretical results exist, empirical behavior—especially on tabular datasets commonly used in practice—remains less clearly communicated.

This short note empirically evaluates the tradeoff between privacy and accuracy when training neural networks with **DP-SGD** using the **Opacus** framework on the UCI Adult Income dataset.

---

2. Experimental Setup

Dataset.
UCI Adult Income dataset (~45k samples after preprocessing). Target is binary classification: income >50K.

Models.

- **Baseline (non-private):**
  2-layer MLP (input → 64 → 1), ReLU, trained with Adam.
- **Private:**
  Same architecture trained with **DP-SGD** using Opacus.

Training details.

- Loss: Binary Cross-Entropy with Logits
- Batch size: 256
- Epochs: 50–100
- Optimizer: Adam (lr = 1e-3)
- DP parameters:
  - Noise multiplier ∈ {0.5, 1.0, 1.2, 2.0}
  - Max gradient norm = 1.0
  - δ = 1e-5

Privacy loss ε is tracked using Opacus' accountant.

---

3. Results

Accuracy vs Privacy

Across a wide range of privacy budgets (ε ≈ 1–8), DP-SGD maintains **~85% test accuracy**, comparable to the non-private baseline.

Key observation:
For sufficiently large datasets, adding calibrated noise does *not* necessarily cause significant accuracy degradation.

Effect of Dataset Size

When limiting the training set to **~3,000 samples**, strong privacy (low ε) leads to a **sharp drop in accuracy**.

This suggests a **data-size × privacy interaction**:

> DP-SGD is considerably more forgiving when sufficient data is available.

---

4. Discussion

These results align with recent empirical findings suggesting that privacy costs are often overestimated in practical regimes. For tabular datasets of moderate size, DP-SGD can preserve strong utility while offering formal privacy guarantees.

However, aggressive subsampling or extremely small datasets amplify the privacy–utility tradeoff, reinforcing the importance of data scale in private learning.

---

5. Limitations & Future Work

- Single dataset and architecture
- No robustness or membership inference evaluation
- Future directions:
    - Repeat experiments across multiple tabular datasets
    - Compare against DP logistic regression
    - Evaluate susceptibility to membership inference attacks
    - Study subgroup accuracy under DP

---

6. Reproducibility

All experiments are reproducible using the public codebase:
GitHub: https://github.com/ShauryaSingh1206/dp-ml-bench