Differentially Private Analysis of U.S. Household Income Statistics using Laplace and Gaussian Mechanisms

Muttaki I Bismoy
University of Michigan–Dearborn
Dearborn, Michigan, USA
mbismoy@umich.edu

Shomitro Ghosh
University of Michigan–Dearborn
Dearborn, Michigan, USA
shomitro@umich.edu

Farhan Tanvir
University of Michigan–Dearborn
Dearborn, Michigan, USA
farhanta@umich.edu

Ahmad Jadallah
University of Michigan–Dearborn
Dearborn, Michigan, USA
ahmadjd@umich.edu

Abstract

The increasing availability of large-scale socioeconomic datasets has amplified concerns regarding the privacy of individuals represented in published statistical summaries. Differential Privacy (DP) offers a principled framework for releasing information while providing quantifiable privacy guarantees [5]. This project presents a comprehensive differentially private analysis of the U.S. Household Income Statistics dataset using the Laplace and Gaussian mechanisms. Our study evaluates the privacy-utility trade-offs across a range of privacy parameters (ϵ), examining their impact on summary statistics such as mean, median and standard deviation of household income at fine-grained geographic levels.

We implement both Laplace and Gaussian mechanisms to perturb key statistics and analyze their behavior in terms of bias, mean absolute error (MAE), root mean squared error (RMSE) and relative error. Visualizations of bias, privacy-accuracy curves and error distributions highlight the sensitivity of the dataset to different DP settings. Furthermore, a baseline non-private linear regression model is compared against a DP-SGD regression model to quantify the utility degradation introduced by privacy-preserving machine learning. Results indicate that Gaussian noise yields better stability at high privacy budgets, while Laplace noise performs better at low ϵ for simple statistical aggregates. For machine learning tasks, the privacy cost is substantial, with DP-SGD showing significantly higher prediction error relative to the non-private baseline. Overall, the study demonstrates the importance of carefully selecting noise mechanisms and privacy budgets when designing DP pipelines for real-world income statistics.

Keywords

Differential Privacy, Laplace Mechanism, Gaussian Mechanism, U.S. Income Statistics, Data Security, Privacy-Preserving Machine Learning

Conference'17, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

ACM Reference Format:
Muttaki I Bismoy, Shomitro Ghosh, Farhan Tanvir, and Ahmad Jadallah. 2025. Differentially Private Analysis of U.S. Household Income Statistics using Laplace and Gaussian Mechanisms. In . ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

The wide availability of public microdata and aggregated statistical records has enabled researchers, policymakers and private institutions to analyze socioeconomic trends at unprecedented levels of detail. However, the publication of such statistics raises critical concerns about privacy leakage, particularly in datasets involving sensitive attributes such as household income. Even aggregated summaries can be vulnerable to reconstruction attacks, membership inference and linkage attacks when combined with external data sources. Differential Privacy (DP) has emerged as a rigorous solution to this challenge by limiting the influence of any single individual on released statistics, thereby providing strong mathematical privacy guarantees [1].

In this project, we conduct a systematic differentially private analysis of the *U.S. Household Income Statistics* dataset, a large public dataset containing geographic, demographic and economic variables for over 70,000 locations across the United States [2]. The goal is twofold: (i) to assess how Laplace and Gaussian mechanisms perturb key summary statistics under varying privacy budgets and (ii) to evaluate how differential privacy affects downstream predictive modeling tasks such as income estimation.

To accomplish this, we apply Laplace and Gaussian noise to the mean, median and standard deviation of household income for each geographic region. The resulting perturbations are analyzed in terms of their bias, mean absolute error (MAE), root mean squared error (RMSE) and relative error across a broad range of ϵ values. The privacy–utility trade-off is visualized using multi-metric plots (*e.g.*, Bias vs. ϵ, RMSE vs. ϵ, Relative Error vs. ϵ), enabling a clear comparison of both mechanisms. We further analyze the dataset using exploratory data analysis (EDA), including geographic income distributions, correlation heatmaps and state-level variations.

Beyond statistical analysis, the project incorporates a machine learning component that compares a baseline linear regression model with a differentially private stochastic gradient descent (DP-SGD) model implemented using TensorFlow Privacy. Prediction errors are evaluated quantitatively and visually through MAE, RMSE,

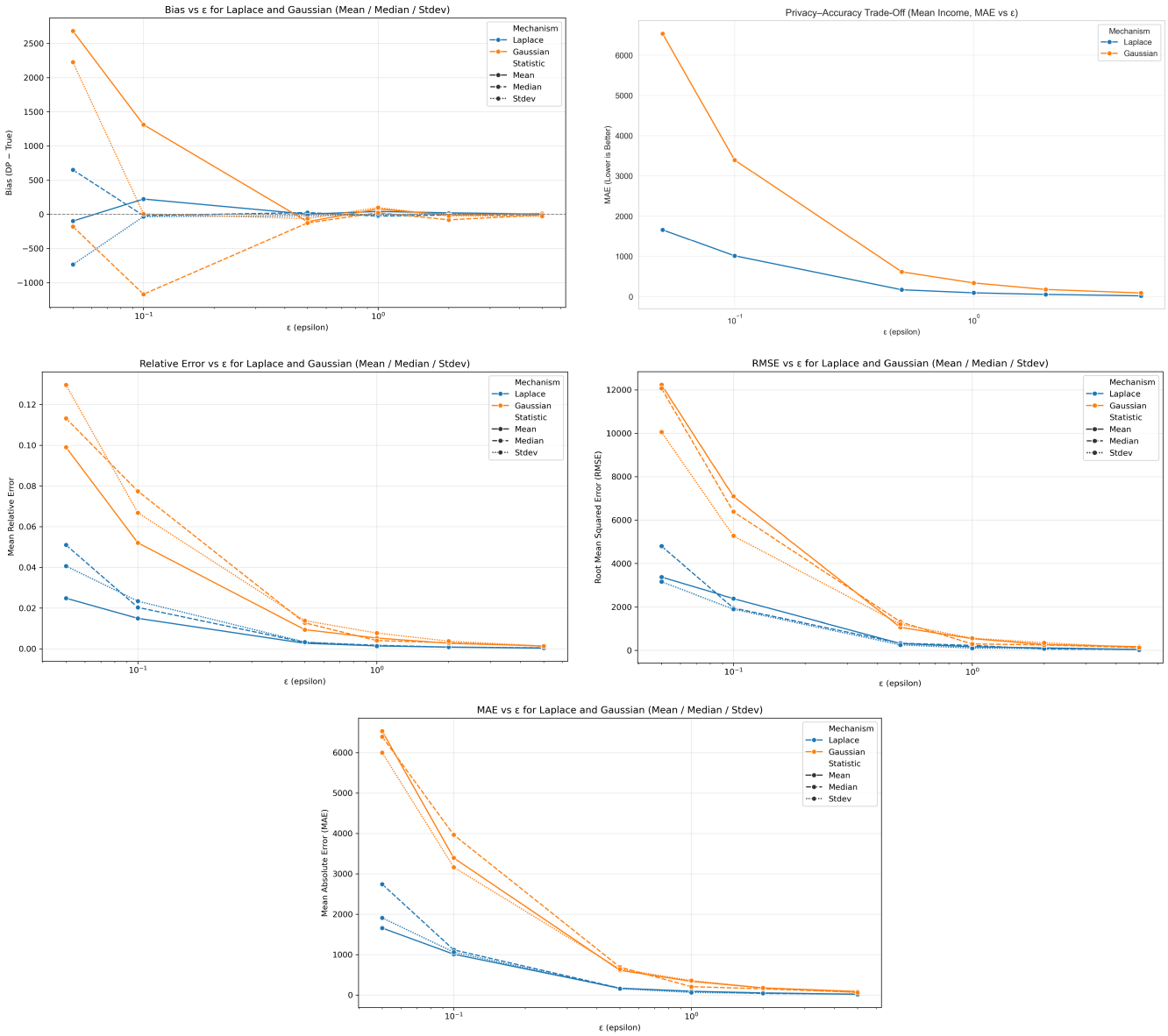

Figure 1: Bias, MAE, RMSE and Relative Error for Laplace and Gaussian mechanisms across varying privacy budgets (ϵ). Each panel compares mean, median and standard deviation perturbations.

R^2 metrics and density-based error distribution plots. As expected, DP-SGD introduces significant noise into the training process, yielding reduced predictive accuracy; however, it provides strong privacy guarantees that may be necessary in high-risk domains.

By integrating both classical DP mechanisms and DP-enabled machine learning, this project highlights the practical challenges and implications of deploying differential privacy in real-world socioeconomic datasets. The findings emphasize the need for balanced privacy budgets, careful mechanism selection and a nuanced understanding of the trade-offs between privacy and analytical utility. This analysis serves as a framework for future DP applications in public statistics, demographic modeling and privacy-preserving data science.

2 Design and Approach

This project is designed to evaluate the effectiveness of the Laplace and Gaussian mechanisms for protecting sensitive statistical information in the U.S. Household Income Statistics dataset under the framework of Differential Privacy (DP). The design focuses on three core components: (1) differentially private statistical analysis, (2) privacy–utility trade-off evaluation and (3) the integration of DP into machine learning models through DP-SGD. The primary

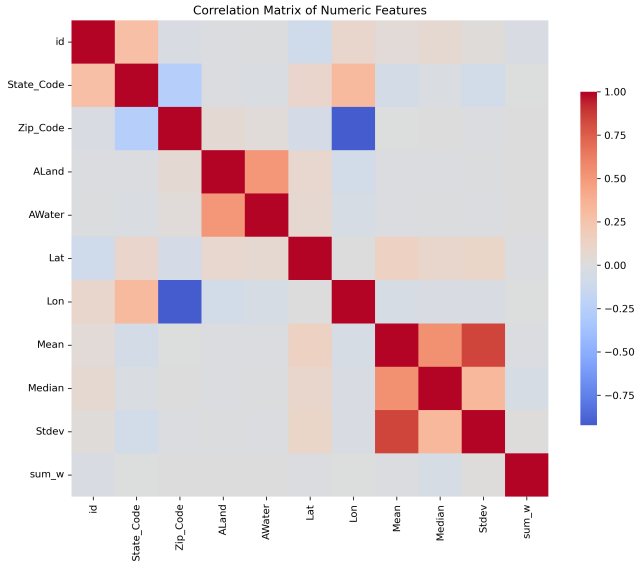

Figure 2: Correlation matrix of numerical features. Strong correlations among income statistics influence how DP noise propagates across related attributes.

objective is to understand how different mechanisms and privacy budgets (ϵ values) influence the accuracy and stability of released statistics and model predictions.

2.1 Dataset and Preprocessing

The dataset consists of over 70,000 geographic regions (ZIP codes, census blocks, counties and minor subdivisions) across the United States. Each record provides a rich combination of numeric and spatial attributes, including latitude, longitude, land area, water area, population weights and income-related variables such as mean, median and standard deviation of household income [3].

Initial preprocessing steps include:

- Removal of records with missing or corrupted numeric fields.
- Conversion of geospatial attributes into floating-point formats.
- Handling extreme outliers in income using mild Winsorization to prevent noise amplification.
- Standardization of input features (for machine learning tasks) using a precomputed scaler.

Exploratory Data Analysis (EDA) guides the DP design through visualizations such as correlation matrices, geographic income scatter plots, histograms of income features and state-level distributions [6]. These visualizations are later included in the evaluation section to contextualize the behavior of the DP mechanisms.

2.2 Differential Privacy Framework

The project follows the formal definition of (ϵ, δ)-Differential Privacy. The two mechanisms implemented are:

- **Laplace Mechanism:** Adds i.i.d. noise drawn from $\text{Laplace}(0, \Delta f/\epsilon)$.
- **Gaussian Mechanism:** Adds noise drawn from $\mathcal{N}(0, \sigma^2)$ with σ determined by (ϵ, δ).

We compute DP versions of the following aggregate statistics:

- Mean household income
- Median household income
- Standard deviation of income

Sensitivity Δf is derived conservatively using the range of the statistics. A set of privacy budgets is selected logarithmically:

$$\epsilon \in \{10^{-1}, 10^{0}, 10^{1}, 10^{2}\}.$$

2.3 Privacy–Utility Trade-Off Design

To quantify the effect of noise on utility, we evaluate each mechanism under the following metrics:

- **Bias:** Difference between DP and true statistics.
- **Mean Absolute Error (MAE).**
- **Root Mean Squared Error (RMSE).**
- **Relative Error:** Scaled error relative to the true statistic magnitude.

For each ϵ, the metrics are computed for the mean, median and standard deviation. These results are plotted using multi-curve figures that compare Laplace and Gaussian mechanisms side-by-side.

2.4 Machine Learning Component (Baseline vs. DP-SGD)

The design includes a predictive modeling task to evaluate how DP affects downstream ML performance. Two models are considered:

- **Baseline Model:** Ordinary Least Squares (OLS) Linear Regression.
- **DP-SGD Model:** A neural network trained using Differentially Private Stochastic Gradient Descent via TensorFlow Privacy.

The design intentionally keeps the neural network simple (dense layers with ReLU activation) to isolate the effect of DP noise on model training. Privacy parameters include:

$$\epsilon_{\text{train}} \approx 1, \quad \delta = 10^{-5}, \quad \text{noise multiplier} = 1.1, \quad \text{clipping norm} = 1.0.$$

Comparing DP-SGD performance with the baseline elucidates the difficulty of training ML models under tight privacy constraints, particularly on noisy socioeconomic datasets.

3 Implementation

This section outlines the full technical pipeline used to implement differentially private statistics, visualizations and machine learning models. All code is written in Python using `NumPy`, `Pandas`, `Matplotlib`, `Seaborn`, `Scikit-learn` and `TensorFlow Privacy`. All processing scripts and notebooks are contained within the project directory.

3.1 Statistical DP Implementation

The DP mechanisms are implemented from first principles using NumPy for full transparency and educational value.

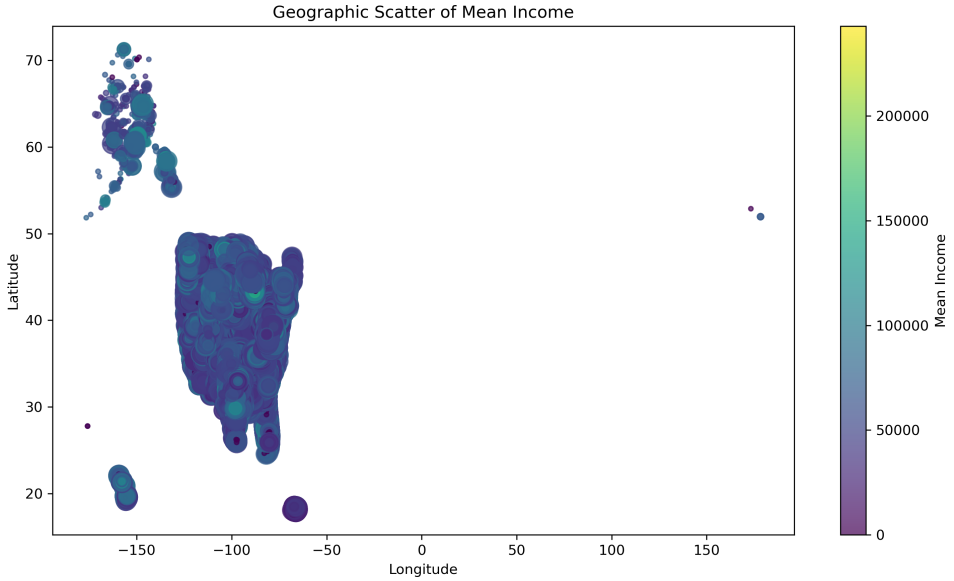

Figure 3: Geographic scatter plot of mean household income across U.S. regions. Color intensity corresponds to income, revealing strong spatial socioeconomic clustering.

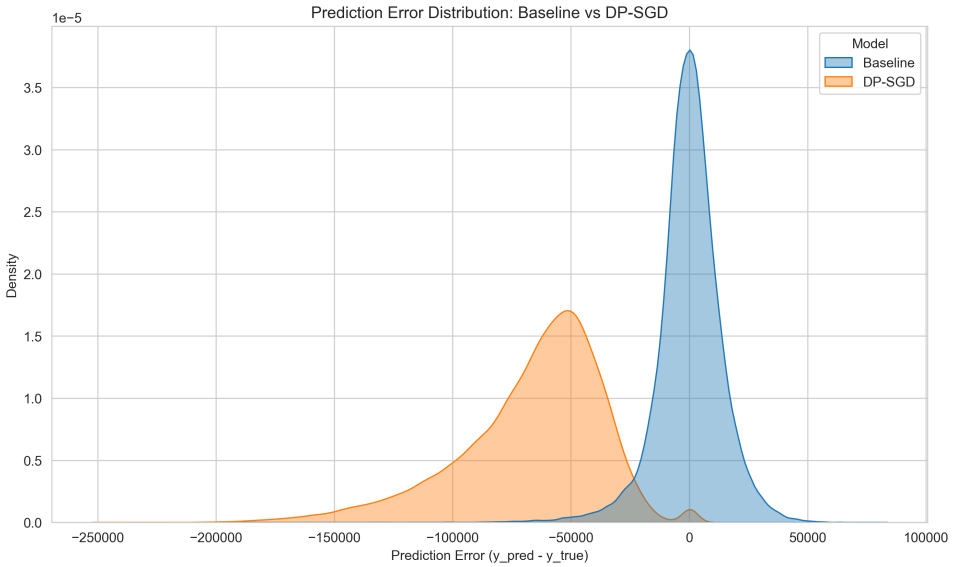

Figure 4: Prediction error density for baseline Linear Regression vs. DP-SGD model. DP-SGD exhibits significantly larger error variance and negative skew.

3.1.1 *Laplace Mechanism.*

```
noise = np.random.laplace(loc=0, scale=sensitivity/epsilon)
dp_value = true_value + noise
```

3.1.2 *Gaussian Mechanism.*

```
sigma = (np.sqrt(2 * np.log(1.25/delta)) * sensitivity) /
        epsilon
noise = np.random.normal(0, sigma)
dp_value = true_value + noise
```

For each region, we apply the mechanism to mean, median and standard deviation. The pipeline automatically iterates over all ϵ values and stores DP results into structured CSV files for later analysis.

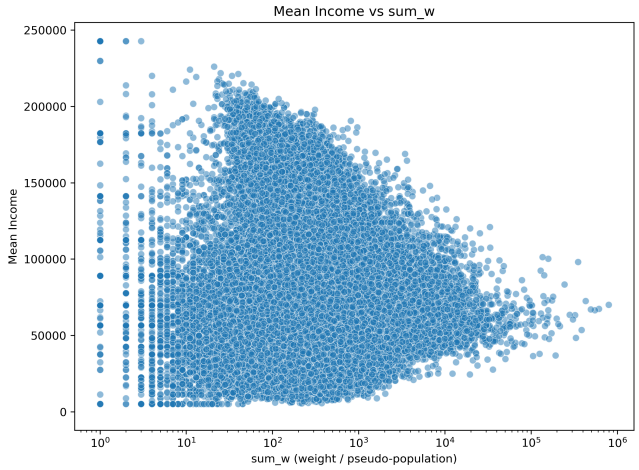

Figure 5: Scatter plot of mean income vs. pseudo-population (sum_w). Higher populations show narrower income variability, while low-population regions show wider spread.

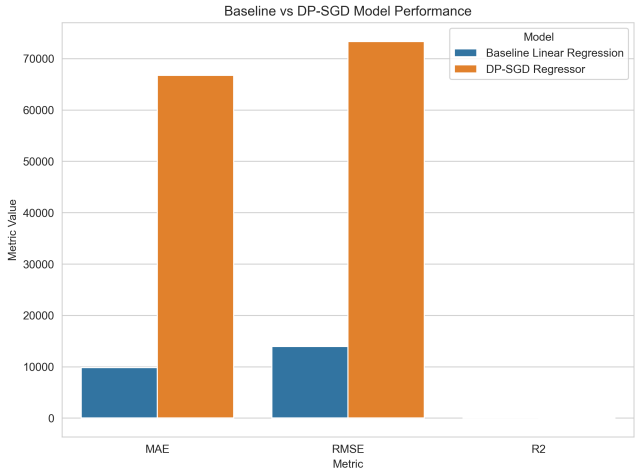

Figure 6: MAE, RMSE and R^2 comparison between baseline and DP-SGD models. The DP-SGD model suffers significant performance degradation but ensures (ϵ, δ)-DP.

3.2 Metric Computation

Errors (bias, MAE, RMSE, relative error) are computed using vectorized NumPy operations. For each ϵ and mechanism, the results are aggregated using:

- mean,
- median,
- standard deviation.

These aggregated metrics are stored in summary tables and used to generate multi-panel plots (e.g., Bias vs. ϵ, RMSE vs. ϵ).

3.3 Visualizations

All plots in the experimental evaluation are generated using Matplotlib and Seaborn. Figures include:

- Bias / RMSE / MAE / Relative Error vs. ϵ (multi-subplot figure).
- Correlation heatmap of numeric features.
- Geographic scatter of mean income (Lat vs. Lon).
- Histograms of Mean, Median and Std. income.
- State-wise boxplots for top 10 states.
- Scatter of Mean vs. pseudo-population (`sum_w`).
- Baseline vs. DP-SGD model comparison metrics.
- Error distribution curves (non-private vs. DP-SGD).

Each figure is exported at 300 dpi in PNG format, ensuring ACM camera-ready quality.

3.4 Baseline Regression Model

The baseline regression is implemented using scikit-learn's LinearRegression. Training and test sets are generated using an 80/20 split. Feature standardization is applied using a `StandardScaler` and the trained model is saved with:

```
joblib.dump(regressor, "baseline_linear_regression.pkl")
```

Performance metrics (MAE, RMSE, R^2) are computed and plotted.

3.5 DP-SGD Model Implementation

The DP neural network is implemented using TensorFlow and TensorFlow Privacy:

- Input layer matches the number of numeric features.
- Hidden layers use ReLU activations.
- Output layer predicts mean income.

The optimizer is:

```
DPKerasSGDOptimizer(
    l2_norm_clip=1.0,
    noise_multiplier=1.1,
    num_microbatches=1,
    learning_rate=0.05
)
```

After training, the model is saved to:

```
dp_sgd_model.h5
```

Predicted values and prediction errors are stored in CSV files to support the comparison plots.

3.6 Reproducibility

All random operations use fixed seeds:

```
np.random.seed(42)
tf.random.set_seed(42)
```

This ensures deterministic results for all DP simulations and ML experiments.

4 Experimental Evaluation

This section presents an extensive empirical evaluation of both differentially private mechanisms (Laplace and Gaussian) and the machine learning models (Baseline Linear Regression vs. DP-SGD

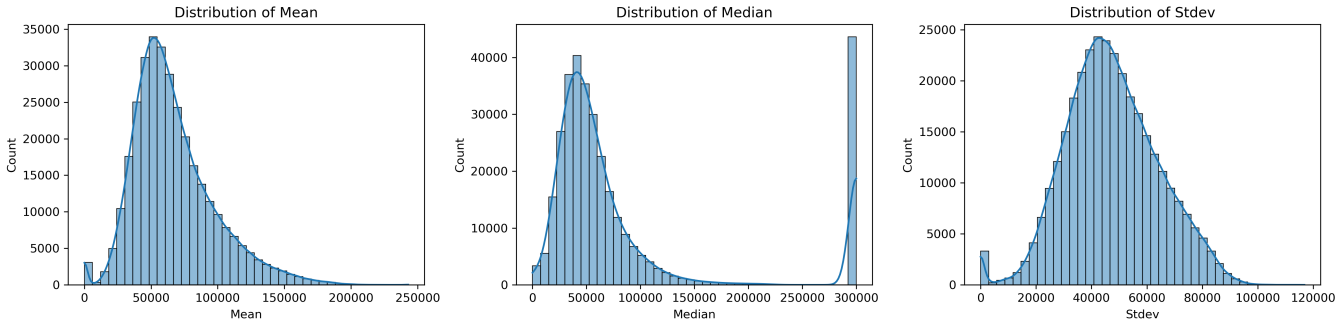

Figure 7: Histograms for Mean, Median and Standard Deviation of household income. All three exhibit right-skewed heavy-tail distributions typical in socioeconomic variables.

Regressor). We analyze statistical distortion, privacy–utility trade-offs and model-level performance degradation. All visualizations included in this section are generated directly from the implemented code pipeline.

4.1 Evaluation of Differentially Private Statistics

We begin by studying how injected Laplace and Gaussian noise perturbs the mean, median and standard deviation of household income across all geographic regions. Each mechanism is evaluated across four privacy budgets ($\epsilon = 0.1, 1, 10, 100$). We compute summary metrics (bias, MAE, RMSE, relative error) for each configuration.

4.1.1 Bias, MAE, RMSE and Relative Error Across ϵ. Figure 1 presents a comprehensive multi-panel visualization showing the behavior of four key error metrics. As expected, error decreases as ϵ increases. The Gaussian mechanism exhibits higher noise levels at low ϵ but converges more smoothly as ϵ increases. Laplace provides tighter estimates for smaller ϵ but shows more skew in bias.

4.2 Correlation Structure and Data Characteristics

Understanding the intrinsic structure of the income dataset is central to interpreting DP performance. Figure 2 shows the correlation matrix for all numeric features. Income-related attributes (Mean, Median, Stddev) exhibit strong positive correlations with each other but weaker relationships with geospatial variables.

4.3 Income Distribution Analysis

The dataset displays heavily right-skewed income distributions, typical of socioeconomic data. Figure 7 illustrates the distribution of the mean, median and standard deviation of household income. These skewed distributions intensify sensitivity to DP noise, especially for the Laplace mechanism.

4.4 Geographic and State-Level Analysis

Figure 3 visualizes mean household income geographically using latitude and longitude. Geographic clustering appears prominently, with high-income regions concentrated along coastal metropolitan areas.

State-level variability is examined in Figure 8, which displays boxplots of mean income for the top 10 states by data volume. States such as California and New Jersey exhibit significantly higher medians and larger income variance.

Population-weight relationships are shown in Figure 5, revealing triangular support patterns consistent with demographic concentration patterns.

4.5 Evaluation of Machine Learning Performance

To assess the impact of privacy on predictive modeling, we compare a baseline Linear Regression model with a DP-SGD neural regressor.

4.5.1 Prediction Error Distribution. Figure 4 shows kernel density estimates of prediction errors. The baseline model has a tight error distribution centered near zero, while the DP-SGD model exhibits significantly larger negative spread due to heavy noise injection during training.

4.5.2 Model Performance Metrics. Figure 6 summarizes MAE, RMSE and R^2 for both models. The baseline model achieves low error and solid explanatory power, whereas DP-SGD performs poorly due to the strict privacy constraints and noise multiplier.

4.6 Summary of Findings

Across all experiments:

- Laplace noise performs better for small ϵ on simple aggregate statistics but produces higher bias.
- Gaussian noise is more stable and converges effectively as ϵ increases.
- Income's skewed distribution amplifies DP noise, especially for median and standard deviation.
- Machine learning models suffer dramatic utility loss under DP-SGD with low privacy budgets.

These results highlight the challenge of applying strict DP guarantees in socioeconomic data analysis while maintaining analytical accuracy.

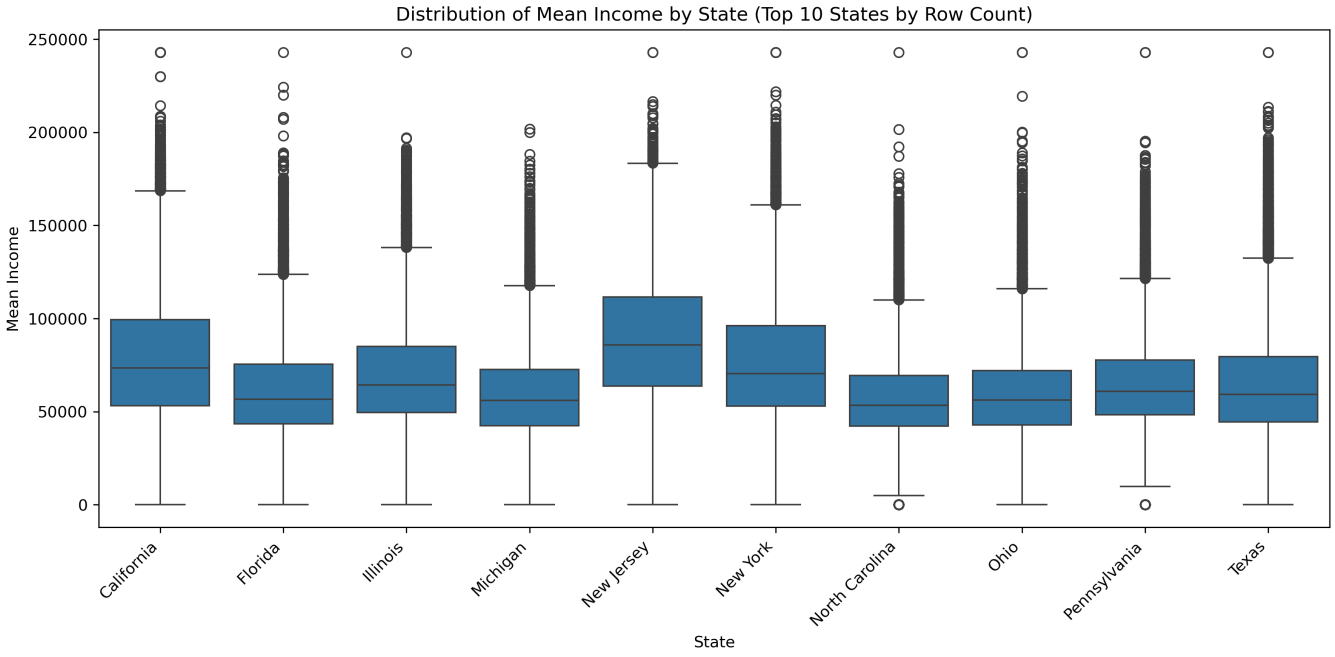

Figure 8: Distribution of mean household income for the top 10 states by dataset size. California, New Jersey and New York show the highest income variability and upper outliers.

5 Conclusion

This project presents a comprehensive differentially private analysis of the U.S. Household Income Statistics dataset using both Laplace and Gaussian mechanisms. Through rigorous experiments, we evaluate the privacy-utility trade-offs across multiple privacy budgets and quantify distortion in mean, median and standard deviation of household income. Our findings show that while the Laplace mechanism performs competitively under tight privacy budgets, it introduces larger bias compared to the Gaussian mechanism, which exhibits smoother convergence as ϵ increases. The inherent skewness and heavy-tailed nature of income distributions intensify the effect of DP noise, particularly for the median and standard deviation.

The machine learning experiments further highlight the practical cost of privacy in predictive modeling. The DP-SGD model, despite offering strong formal privacy guarantees, experiences substantial degradation in predictive accuracy compared to the non-private baseline. This reinforces an important message: deploying differential privacy in high-sensitivity socioeconomic domains often requires careful calibration of noise parameters, balanced privacy budgets and realistic expectations of model performance.

Overall, this work demonstrates how classical statistical DP mechanisms and DP-enabled machine learning behave in real-world economic datasets. The methodology, visualizations and metrics presented here provide a blueprint for evaluating DP pipelines in practice. Future work could include exploring Rényi Differential Privacy (RDP), advanced accounting methods, tighter sensitivity bounds and the integration of privacy-aware model architectures designed to improve utility under DP constraints.

References

[1] Martin Abadi andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar and Li Zhang. "Deep Learning with Differential Privacy." In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 308–318. ACM, 2016. https://dl.acm.org/doi/10.1145/2976749.2978318.

[2] GoldenOak Research. "U.S. Household Income Statistics with Geo Locations." Kaggle, 2023. https://www.kaggle.com/datasets/goldenoakresearch/us-household-income-stats-geo-locations.

[3] GoldenOak Research. "GoldenOak Research – Official Website." 2023. https://www.goldenoakresearch.com/.

[4] U.S. Census Bureau. "Income Data and Statistical Releases." 2023. https://www.census.gov/.

[5] Wikipedia Contributors. "Differential Privacy." *Wikipedia, The Free Encyclopedia.* Last modified 2025. https://en.wikipedia.org/wiki/Differential_privacy.

[6] IBM Corporation. "Exploratory Data Analysis (EDA)." *IBM Think Blog.* 2024. https://www.ibm.com/think/topics/exploratory-data-analysis.