**Feedback**: The Effects of Privacy Protection on Forecast Accuracy

1. It seems easy to adjust for top-/bottom-coding using a censored model. Rather than saying “…use RNN,” it would be more valuable to study how to “undo” the data protection based on what knowledge is available of the data protection method.
   1. Saying “… use RNN,” is more defensible if we claim the forecaster does not have knowledge of the data protection method. This is an unrealistic assumption – either the data provider discloses the privacy protection measures that were applied to the data, or the forecaster can likely identify top-/bottom-coded vs. differentially privacy data. That being said, I want to study the ‘nuts and bolts’ of how and why model performance is affected by data protection. This would inform future work on improving model performance under data protection.
   2. I plan to continue with a focus on explaining why models do well or poorly (see points II and IV below). I will remove the table that averages across data protection methods and says to just use RNN, and instead focus on which models do best under each protection method. While we aren’t showing how to *adjust for data protection*, we can provide evidence on which models perform best with a ‘naïve’ application to protected data and suggest future research on improving model performance on protected data.
2. Examine the distribution of forecast errors, not just the mean.
3. Pierre: look at distribution of errors.
4. Pierre: interested in data sharing markets.
   1. I like this idea. Average accuracy is important, but to have confidence that all of your forecasts with protected data are reasonably accurate, you also want low variance in forecast error.
   2. I plan to compare the error distributions of each model under each protection model using variance and graphical comparisons. We might identify cases where it is preferable to use a model that has slightly worse MAE, but low forecast error variance. Since we are forecasting with protected data, models with a high forecast error variance would be very worrisome because forecasters don’t know which series have low vs. high error.
5. It’s clear that differential privacy results in terrible forecast accuracy. You should consider matrix-based methods as well.
   1. This was advice from Pierre Pinson. I’m not 100% sure what is meant by matrix-based methods here.
   2. I need to do some literature review on this. If I can figure out which matrix-based methods are applicable to our scenario (single data owner, forecasting for multiple time series) I will implement one for comparison.
6. Using decision tree/random forest to classify judgmental (privacy adjusted) forecasts.
   1. [this paper](https://www.sciencedirect.com/science/article/abs/pii/S0377221722002260?casa_token=un4vxuF7kPUAAAAA:mFGEjjQrWOVhvMTL7M8FDuVGAPP7Nd8RR6GpNaIt6BCECf8evNMA6YKNpwxqVD8nEyPbmX1H_Q) uses a random forest to identify the drivers of adjustments and their quality
   2. Then, they use decision trees to identify the effects of drivers of adjustments on the occurrence and quality of the adjustments.
   3. I want to use a similar approach. We should be able to classify which time series have improved/worsened accuracy under each protection method and explain these predictions using time series characteristics.
7. Techniques for explaining ML/DL model Forecasts
   1. I have found a few resources that might help us in this area and I will be doing a closer review of them soon.
      1. Performance-based shapley values
         1. These were presented as ISF, and identify which data features contribute most to forecast (not training data) accuracy. I have spoken to one of the authors who said a working paper will be available in the coming weeks with equations to help with code implementation.
      2. WeightWatcher: Empirical quality metrics for deep neural networks
         1. [This blog](https://calculatedcontent.com/2020/02/16/weightwatcher-empirical-quality-metrics-for-deep-neural-networks/) describes the weightwatcher framework which can assess the quality of neural network models.
         2. I plan to look through this work more closely, I’m still not sure if it is applicable. I’m hoping it could help us say something about the weight matrices of the neural network and how that translates into forecast accuracy.
      3. Other methods of comparing neural network similarities to understand performance (see attached paper).
8. Timeline
   1. Finish analysis and paper rough draft for current dataset by **9/23/2022.**