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

1. **Introduction**

Forecasting is popular in a variety of fields, such as consumer analytics, renewable energy and power industries, and census tracking, all of which may benefit from the use of commercially or personally sensitive data. Examples include using social media information (Boone et al., 2019) and collaboratively shared power generation data (Gonçalves et al., 2021) to improve forecast accuracy. The privacy concerns associated with sensitive data have been demonstrated across many domains. Data ranging from consumer locations (de Montjoye et al., 2013) to smart meter usage (Véliz & Grunewald, 2018) can be used to identify individuals and/or infer sensitive information about them. Furthermore, a large number of privacy laws such as the General Data Protection Regulation (GDPR)[[1]](#footnote-1) require organizations to protect their sensitive data to avoid fines.

Various protection approaches are available depending on whether time series are stored in a single data set or spread across multiple data owners/data sets. In the multiple data owners scenario, multi-party computation or federated learning enable privacy-preserving collaborative forecasting to ensure accurate forecasts while protecting sensitive data (Gonçalves et al., 2021; Goncalves, Bessa, et al., 2021; Sommer et al., 2021). On the other hand, we focus on scenarios in which a single data owner uses privacy methods to protect a time series data set. These privacy methods alter the sensitive data to produce protected time series which limit the ability of a bad actor to identify data subjects and learn sensitive information about them. One example is the Census’ use of random noise to perturb the individual and business level data that goes into calculating Quarterly Workforce Indicator data (Abowd et al., 2012). Privacy methods are attractive to organizations since when applied correctly, the data produced by these methods can be exempt from privacy laws[[2]](#footnote-2). The concern for forecasters is that privacy methods can drastically alter time series, leading to privacy adjusted forecasts. Empirical evidence of the effects of privacy methods on forecasts and the reasons behind changes in forecast accuracy would help forecasters adapt to using protected data.

While it has been demonstrated that differential privacy degrades forecast accuracy for VAR models and recurrent neural networks (RNNs) (Gonçalves et al., 2021; Imtiaz et al., 2020), there is no work which compares how multiple forecasting models perform on protected data. This comparison is needed because different forms of data protection produce different data points which will ultimately have different forecasts than what would be produced based on the original data. This paper provides an empirical analysis of forecasting with protected data. First, we investigate the drivers of changes in forecast accuracy for protected data. Specifically, we examine time series characteristics that give insight into why forecast accuracy changes. We develop a new matrix-based privacy method which swaps the values of time series with similar characteristics to balance the trade-off between privacy and forecast accuracy. We provide empirical results of forecast accuracy for protected data and examine model-specific behavior to understand why certain models perform better than others. Motivated by findings from the judgmental forecasting literature, we investigate characteristics of privacy adjusted forecasts with improved forecast accuracy and assess the parallels between privacy and judgmentally adjusted forecasts.

The rest of the paper proceeds as follows…

1. **Lit Review**

Some forecasters have studied data privacy and forecasting in the context of collaborative forecasting. (Goncalves, Pinson, et al., 2021) explored a data market where data owners are compensated for sharing their data, and purchase forecasts based on the data from other parties. While data owners have a monetary incentive to share their data, they may be discouraged from doing so due to privacy concerns over sharing data with a central party. In such a situation, our work would help answer how forecast accuracy would be affected if the data owners applied data protection methods prior to sharing their data in the market. In the absence of a data market, other privacy-preserving solutions for collaborative forecasting include secure multi-party computation, decomposition-based methods, and data transformation techniques, all of which are succinctly described by (Gonçalves et al., 2021).

Our interest is in privacy methods which generate protected data sets. The first methods we consider, known as additive or multiplicative noise and differential privacy, are based on incorporating random noise into the data. Given a confidential time series , a differentially private time series can be created using a randomized mechanism which adds Laplace random noise with scale parameter . The sensitivity is determined as the maximum absolute difference between two time series and , which differ in at most one observation, where . The mechanism satisfies -differential privacy by guaranteeing that, for every output of and every pair of series and ,

.

Using this definition, (Gonçalves et al., 2021) show that differential privacy reduces the forecast accuracy of VAR models even under very high values of the privacy parameter (weak privacy protection). Others have also studied the application of differential privacy to time series (Imtiaz et al., 2020; Liyue Fan & Li Xiong, 2014). Additive and multiplicative noise infuse random noise in the data but without the theoretical privacy guarantees of differential privacy. While (Abowd et al., 2012) study the use of multiplicative noise, they do not offer forecast accuracy results. Through simulated data integrity attacks, however, we know that multiplicative noise reduces forecast accuracy (Luo et al., 2018).

One interesting result from (Imtiaz et al., 2020) is that differentially private data did not always produce worse forecast accuracy when forecasting individuals' health data using a recurrent neural network. Adding random noise to time series mirrors a technique used to prevent overfitting when forecasting with neural networks (Hewamalage et al., 2021, 2022). We explore whether data protection with random noise can achieve this same regularization at meaningful levels of privacy.

Another type of privacy method is generalization, where data records are generalized to create equivalence classes of identical records. This privacy method is particularly popular for tabular data. The principle of *k-*anonymity (Sweeney, 2002) is used to describe when every record (or time series) is identical to at least other records on a pre-determined set of attributes (or time periods). (Nin & Torra, 2009) evaluate the change in forecast accuracy for simple exponential smoothing, double exponential smoothing, linear regression, multiple linear regression, and polynomial regression applied to *k*-anonymized data. The authors find an overall reduction in forecast accuracy even for but do not provide the accuracy of each model individually.

There are also privacy methods which are commonly used in practice but have not been studied in the forecasting literature. Top- and bottom-coding are used to replace the top (bottom) *p* percent of observations with the quantile. These methods are useful for protecting data with sensitive values in the tails of distributions, such as income levels or smart meter data. (Crimi & Eddy, 2014) study the effect of top coding the Census’ Public Use Microdata Samples on analyses of interest. They find that the sample correlation between two variables is shrunk towards zero when one or both of the variables are top coded. This may be relevant to multivariate forecasting model accuracy, which relies on the correlations between time series, and may be negatively affected when series are top- or bottom-coded. On the other hand, top- and bottom-coding could have an effect similar to adjusting for outliers, which can improve forecast accuracy when the outliers are close to the forecast origin (Chen & Liu, 1993).

Overall, while recent attention has been paid to privacy preserving collaborative forecasting, our interest is in forecasting using a single protected dataset. There has been no work which compares multiple forecasting models' accuracies when forecasting for a single protected dataset, or a comparison of models' accuracies under various privacy methods. The works which have shown that data protection degrades forecast accuracy have also not given detailed explanations as to why model performance is worse on protected data. Finally, there exist no privacy methods which are specifically designed with forecasters in mind, which our work remedies.

* 1. *Privacy Adjusted Forecasts*

Judgmental adjustments to forecasts can improve accuracy by accounting for information that was not incorporated into a forecasting model (Fildes et al., 2009). Incorporating the intuition and experience of the adjuster, knowledge of special events, or insider or confidential information can add information with high diagnosticity that is useful for forecasting. However, adding information with low diagnosticity can degrade forecast accuracy (Fildes et al., 2019). Adjusting forecasts for the sake of gaining control of the forecasting process, incorporating practitioner expectations, and compensating for judgmental biases can be detrimental to forecast accuracy ((Petropoulos et al., 2022) section 3.7.3). Despite varying motivations for judgmentally adjusting forecasts, these adjustments have been found to improve the accuracy of monthly demand forecasts from statistical models by an average of 10% (Davydenko & Fildes, 2013). The accuracy improvements are greater for low volatility time series which are easier to forecast (Fildes et al., 2009).

The characteristics of adjustments have an effect on forecast accuracy. Both positive and negative adjustments can improve accuracy, but positive adjustments tend to give only a marginal improvement (Davydenko & Fildes, 2013). Forecast bias can be reduced by negative adjustments, whereas positive adjustments maintain bias or exacerbate it (Fildes et al., 2009). The magnitude of judgmental adjustments is positively associated with the size of accuracy improvements, which can occur when larger adjustments are made by adjusters who are confident in reliable information (Fildes et al., 2009).

The reasons for applying privacy methods are varied as well. Privacy legislation places strict limitations on data transfers and processing[[3]](#footnote-3) which can hurt business performance. For example, (Goldfarb & Tucker, 2011) found that privacy regulation in the European Union led to a 65% average reduction in banner ad effectiveness at influencing purchase intent. Legal limitations can be circumvented when data is properly protected, but this comes at the cost of reducing the utility of the data. Data from regulated domains, such as healthcare (HIPAA) and finance[[4]](#footnote-4) must also be protected. Other reasons for implementing privacy methods include reducing consumers' privacy concerns (Martin et al., 2017) or attempting to gain a competitive advantage through privacy-conscious brand positioning (Goldfarb & Tucker, n.d.). Several of the largest tech companies in the world, including IBM, Google[[5]](#footnote-5), Meta, and Microsoft[[6]](#footnote-6) implement privacy methods and provide open-source code to enable others to do the same. Notably, Apple has positioned themselves as a privacy-focused company[[7]](#footnote-7).

Regardless of the motivation for data protection, privacy adjusted forecasts arise from changes to the data, which are made without regard to the effects on forecast accuracy. Privacy methods based on random noise add information with low diagnosticity, and are likely to reduce forecast accuracy. While the direction of adjustment is purposefully chosen in judgmental forecasting, the direction of privacy adjustments will occur indirectly via data protection. Under data protection, the adjustment size will again be determined by the forecasting models' responses to data protection. These responses are likely related to the strength of data protection, where stronger data protection results in larger changes to the data.

Data protection will affect time series characteristics that are important for forecast accuracy, which we can use to understand why accuracy changes under data protection. There are thousands of time series features which have been used for time series classification (Fulcher & Jones, 2014). A smaller set of interpretable features was used by (Bandara et al., 2018) for clustering and forecasting similar time series, which improved the accuracy of recurrent neural network models. Our focus is on features which are predictive of forecast accuracy, since privacy methods which alter these features will be most detrimental for forecasting.

The initial results from the M4 competition suggested that the randomness and linearity of time series were the most important determinants of forecast accuracy, and that seasonal time series (which are typically less noisy) are easier to forecast (Makridakis et al., 2018). In a follow-up study, (Spiliotis et al., 2020) confirmed the importance of randomness, linearity, and seasonal strength in predicting the MASE values of the ETS, ARIMA, Theta, and Naïve 2 (random walk applied to seasonally adjusted data) models from the M4 competition. On average, increasing the frequency, kurtosis, linearity, and seasonal strength of time series contributed to improved forecast accuracy. However, increasing skewness, self-similarity, and randomness affected accuracy negatively. While strength of seasonality improved the accuracy of all models, strength of trend had no statistically significant effect on accuracy for ETS, ARIMA, and Theta, while hurting accuracy for Naïve 2, which has no means of accounting for trend.

Outside of predicting forecast accuracy, time series characteristics such as strength of trend and seasonality and the spikiness of series have been used in exponential smoothing model selection (Qi et al., 2022). Forecasts based on this feature-based model selection had lower MASE, sMAPE, and MSIS than information-based selection methods for the majority of forecast horizons. Time series characteristics have also been used to select optimal model and forecast combinations (Li et al., 2022; Talagala et al., 2022). Model selection based on the representativeness of forecasts (Petropoulos & Siemsen, 2022) selects models with trend and seasonality components when the respective signals of these components are strong, and has been shown to outperform information criteria-based and cross-validation based model selection.

Our contributions are two-fold. First, we analyze privacy adjusted forecasts for multiple forecasting models and privacy methods, giving detailed explanations as to why model performance changes on protected data. To explain the improvement and/or degradation of forecast accuracy from data protection, we analyze privacy adjusted forecasts from two perspectives: (1) How data protection changes time series characteristics which translate into changes in forecast accuracy, and (2) How changes to forecasts are related to changes in forecast accuracy. To address (1), we extract time series features which are predictive of forecast accuracy and show how these features change under data protection. This examination informs why certain models perform better than others on protected data. To address (2), we measure whether forecasts are positively or negatively adjusted under data protection as well as the magnitude of each adjustment. Similar to (Fildes et al., 2009) and (Khosrowabadi et al., 2022), we classify privacy adjusted forecasts as either improving or degrading forecast accuracy. We use the random forest approach of (Khosrowabadi et al., 2022) to identify the time series characteristics and adjustment features that are predictive of whether privacy adjusted forecasts improve or degrade accuracy.

For our second contribution, we propose a novel privacy method designed with forecasters in mind. We implement a matrix-based privacy method which swaps the values of time series with similar characteristics to help maintain forecast accuracy. Results show that our method... We describe our proposed method next.

1. **The *k*-nearest Time Series (nTS) Swapping Method**

See attached pdf.

1. **Empirical Application**
   1. *Data*

Recent work by (Spiliotis et al., 2020) showed that the M3 competition data are representative of the real world on the basis of time series characteristics. Complex forecasting models are known to forecast more accurately than simple models using the unprotected version of the M3 competition monthly micro data (Koning et al., 2005), and models that explicitly capture trend and seasonality performed the best in the overall M3 competition (Makridakis & Hibon, 2000). We are interested in whether these results hold when forecasting using protected versions of the data. For our analyses, we use the monthly micro dataset from the M3 competition, which includes 474 strictly positive time series with values ranging from 120 to 18,100. Of the 474 series, 18 consist of 67 time periods, 259 consist of 68 time periods, and 197 consist of 125 time periods.

* 1. *Privacy Methods*

Graphical user interface, application, Word

Description automatically generated

We apply each of the privacy methods shown in the table below to the original M3 monthly micro data for each of the displayed parameter values. For *k*-nTS, the distance between time series is calculated using the nine features described in Section 4.3.

Graphical user interface, application

Description automatically generated

We assume each protected dataset consists of each protected series along with the associated pseudo identifier, i.e., . To assess the privacy of the protected datasets, we assess the risks of *identification disclosure* and *attribute disclosure*.

We define identification disclosure in the context of a third party which possesses some external data pertaining to a unit in the protected dataset. Denote this external information which contains a direct identifier and confidential data which contains a subset of confidential values , and that the first of these values occurs in time period .

We let denote the random variable that indicates the corresponding for , i.e., when the confidential data in corresponds to protected series . Identification disclosure occurs when the third party identifies this correspondence, thereby identifying a unit of interest in the protected data set. For simplicity, we assume the third party does not know which privacy method was applied to the data and knows that the unit of interest is contained in the protected data set.

The identification attack proceeds as follows. Let denote the protected values of each time series that begin in time period . The third party computes the distance between and the protected values using the Euclidean distance,

and computes the similarity between and as

.

Using the similarities , the third party builds a probability mass function for over all the series in as

We let denote the probability that is correctly matched to . The third party predicts the value of to be the protected time series with the maximum match probability,

.

To estimate the risk of identification disclosure of a protected dataset, we sample sequential values at random from each confidential time series and treat these as external information . Each of the external data vectors corresponds to one of the confidential time series and we compute conditional on the sampled from series . We repeat this process to obtain , and compute

which is the average probability of correct identification across all external data samples for each confidential time series. A second measure of identification risk is

where [.] are iverson brackets. This measure gives the average proportion of correctly identified time series across all external data samples.

To perform attribute disclosure, we assume the third party predicts additional confidential values for each series based on the known confidential values and the predicted match, i.e., the -th protected time series. For our purposes, we assume the third party is interested in the confidential value that immediately follows the known confidential values, i.e., The third party regresses the known confidential values in on the corresponding protected values from each matched series,

(1)

and predicts the unknown confidential value of each time series in time period based on the protected value from that period,

(2)

To estimate the risk of attribute disclosure in a protected dataset, i.e., the risk of the third party correctly predicting the confidential value of each time series in time period , we perform the regression and prediction steps (1) and (2) for each , and measure the average MAE of the third party’s predictions across all samples,

* 1. *Time Series Features*

In this section, we describe the time series features which have been demonstrated to have a relationship with forecast accuracy. We let denote a univariate stationary time series with a finite mean and constant variance. The spectral density of is estimated as the scaled fourier transform of the autocovariance function of . The spectral density can be thought of as the probability density function of a random variable on the unit circle (Goerg, n.d.), where for a non-zero integer , when , the spectral density will have a peak at the corresponding frequency . The forecastability, or spectral entropy, of is measured using the Shannon entropy of , given by

Graphical user interface, application, Word

Description automatically generated

,

where the maximum entropy is attained when . In practice, estimates of , where high values represent a low signal-to-noise ratio, indicating that is difficult to forecast (Kang et al., 2017).

Next, we consider the self-similarity feature quantified using the Hurst parameter (Wang et al., 2006), which measures the long-range dependence of a time series. This feature had the largest magnitude effect on forecast accuracy in the study of the M4 data performed by (Spiliotis et al. 2020). We use the definition of self-similarity of a time series described by (Willinger et al., n.d.). Suppose that is the increment process of , i.e.,

An aggregated sequence, denoted , is created by averaging over non-overlapping blocks of size , where

and indexes the block. If is a self-similar time series, then

for all integers . We focus on the definition of second-order self-similarity, where is exactly second-order self-similar if has the same variance and autocorrelation as for all values of , or is asymptotically second-order self-similar if this holds as (Rose, n.d.). The parameter is the Hurst exponent, which is estimated using the differencing term from a fractional ARIMA model, i.e., FARIMA(0, , 0) (Wang et al., 2006) (Hyndman et al., 2022), where

.

Estimates of fall in the interval (0, 1), where corresponds to a random walk (Sobolev, 2017), corresponds to anti-persistent or mean-reverting series, and corresponds to persistent time series that are more likely to maintain their current trend. (Rose, n.d.) notes that a self-similar process has a spectral density that follows a power law near , where as with . When , the spectral density increases rapidly as and will tend to have low spectral entropy, whereas when , the spectral density increases slowly as and will tend to have high spectral entropy. For a random walk with , i.e., the spectral density is finite at the origin (Rose, n.d.).

We consider the remaining features from (Spiliotis et al., 2020) which had the largest effects on forecast accuracy. Since none of the privacy methods we consider will change the time series’ frequency, we omit this feature from consideration, noting that higher frequencies are associated with improved forecast accuracy. We include skewness and kurtosis which measure the shape of the distribution of time series’ values.

Skewness, which we denote , measures the lack of symmetry in the distribution of the values of (Wang et al., 2006), where positive (negative) values are associated with a right- (left-) skewed data distribution:

.

We use a measure of Kurtosis relative to the standard normal distribution (Wang et al., 2006). Positive kurtosis corresponds to distributions that tend to have a distinct peak near the mean with heavy tails, whereas negative kurtosis corresponds to distributions that are relatively flat near the mean,

where 3 is the kurtosis of the standard normal distribution.

Next, we perform STL decomposition (Cleveland et al. 1990) to obtain the trend, seasonal, and remainder components of . We use the approach of (Hyndman et al. 2019) which is designed to handle multiple seasonalities to obtain

,

where , , and are the trend, Seasonal, and remainder components, respectively.

We extract the first order autocorrelation coefficient of the detrended and deseasonalized series, referred to as ‘linearity’ by (Spiliotis et al. 2018).,

gives a measure of the forecastability of a time series after the trend and seasonality have been accounted for.

,

.

In practice, the values of are bounded to (Hyndman 2022).

Our final two features are included to maintain data utility throughout the *k*-nTS swapping process. The idea is to swap values between series that not only have similar characteristics, but whose values have similar magnitudes. Toward this end, we include the mean and the variance of ,

.

* 1. *Forecasting Models*

In this section, we introduce the forecasting models which we apply to the original and protected data. The models are separated into “simple” models which are trained to forecast one series at a time, and “complex” models which are trained to generate forecasts for multiple series. For all models, we perform minimal data pre-processing, and allow the models to capture the important components of the series. Our goal is to assess the effects of privacy protection on the accuracy of popular forecasting models which are readily available to implement in R and/or Python and have served as benchmarks or winners in recent forecasting competitions. Please see the appendix for full implementation details, including hyperparameter optimization for the complex models.

* + 1. *Simple Models*

We consider four simple models. The first is single exponential smoothing (SES), which can be written as follows:

Graphical user interface, application, Word

Description automatically generated

where is the level of the series at time and is the smoothing parameter for the level. The forecast for a given period is a weighted average of the last known observation and the previous level . High values of place more importance on recent observations when generating forecasts, whereas low values of place more importance on older observations. SES is suitable for series that do not exhibit trend or seasonality.

* + 1. *Complex Models*

We also consider three complex models. The first is a variant of the VAR model known as VARX-L (Nicholson et al., 2017), which we fit using the BigVAR package in R. Fitting large VAR models is already computationally expensive since the number of estimated coefficients is where is the number of series and is the number of lags. The problem is compounded in our case since we have fewer time periods than series. We use the VARX-L model which implements the Lasso penalty to induce sparsity in the coefficients and enable model estimation and fit one VAR model to each subset of series with the same length, resulting in three VARX-L models being estimated per data set.

The second complex model we consider is a light gradient boosted machine (LGBM) (Ke et al., n.d.), which was the top performing model in the M5 competition (Makridakis et al., 2022). This is a global forecasting model trained on all time series in our data set.

Our final complex model is an RNN with long short-term memory cells (LSTM). This model was a component in the winning solution to the M4 competition (Makridakis et al., 2018; Smyl, 2020). Similar to the LGBM, the RNN is a global forecasting model.

1. **Results**
   1. *Relationships Between Time Series Features*

**FIG 1 (Scatterplot matrix showing scatterplots between each feature pair, kernel density of each feature, and correlations between each feature pair for the original data.)**

Diagram

Description automatically generated

In the upper triangle of **FIG 1**, “\*\*\*” denotes p-value < 0.001, “\*\*” denotes p-value < 0.01, “\*” denotes p-value < 0.05, “.” denotes p-value < 0.10, “” is shown otherwise.

Most interesting results:

* Spectral entropy distribution is skewed left, approximately 63% of series have a spectral entropy of at least 0.75 (a lot of series are already difficult to forecast)
  + Spectral entropy for which higher values indicate worse forecastibility, is negatively correlated with features that improve forecastability such as Hurst exponent, strength of trend and seasonality, and remainder first autocorrelation coefficient (e-acf1).
  + Strongest negative correlations are between spectral entropy and Hurst exponent (-0.786) and strength of trend (-0.830)
  + For this data, series with a higher mean tend to have higher spectral entropy (cor = 0.310).
* Hurst exponent density is bi-modal with peaks near 0.5 and 1
  + Larger Hurst exponent (and smaller spectral entropy) indicate there are stronger auto-correlations and strength of trend and seasonality (notice correlation of 0.926 between Hurst and strength of trend). Increasing strength of trend and seasonality indicates that more of the variance of a series is due to these components, rather than the remainder.
    - The findings in (Spiliotis et al., 2020) suggest that after controlling for spectral entropy and strength of trend, increasing the Hurst coefficient actually harms accuracy – why?
* Skewness distribution is roughly symmetric with slight tendency toward negative values
  + Strongest correlations are with Variance (-0.33) and seasonal strength (0.33)
    - Increasing the value of skewness is associated with lower variance – based on the scatterplot between Variance and skewness, the left-skewed series tend to have higher variances
    - The right-skewed series tend to have stronger seasonality
    - If we consider the absolute value of Skew, there is no correlation between skewness and spectral entropy for this data
* Kurtosis distribution has a large right-skew, indicating that there are some series that are peaked near the mean, but have fat tails
  + Kurtosis is most strongly correlated with spectral entropy (0.287), where increased Kurtosis is associated with increased spectral entropy – harder to forecast fatter tails
  + Kurtosis has weak negative correlations with Hurst exponent, strength of trend, and strength of seasonality, again indicating increased difficulty in forecasting series with high kurtosis
  + Based on the scatterplot between Kurtosis and Skewness, the series that are most skewed have the highest Kurtosis values
* Strength of trend is positively correlated with other features that improve forecast accuracy: Hurst, strength of seasonality, e-acf1
* Mean distribution is roughly symmetric
  + Strong negative correlation (-0.55) with variance – series (in this data) with a larger mean tend to have lower variance and be less forecastable
* Variance distribution has a strong right skew
* E-acf1 is roughly symmetric, with mean of -0.115
  1. *Changes in Time Series Features from Data Protection*

We quantify the effect of each privacy method on the time series characteristics using the Kullback-Leibler divergence between the distribution of each feature calculated from the protected series and the distribution of each feature calculated from the original series.

The Kullback-Leibler divergence between two probability densities and is defined as

f

where is the probability density of the original feature, and the probability density of the feature from the protected data is denoted . Following the approach of (Spiliotis et al., 2020), we approximate and using normalized kernel densities, and estimate the KL-divergence between and as

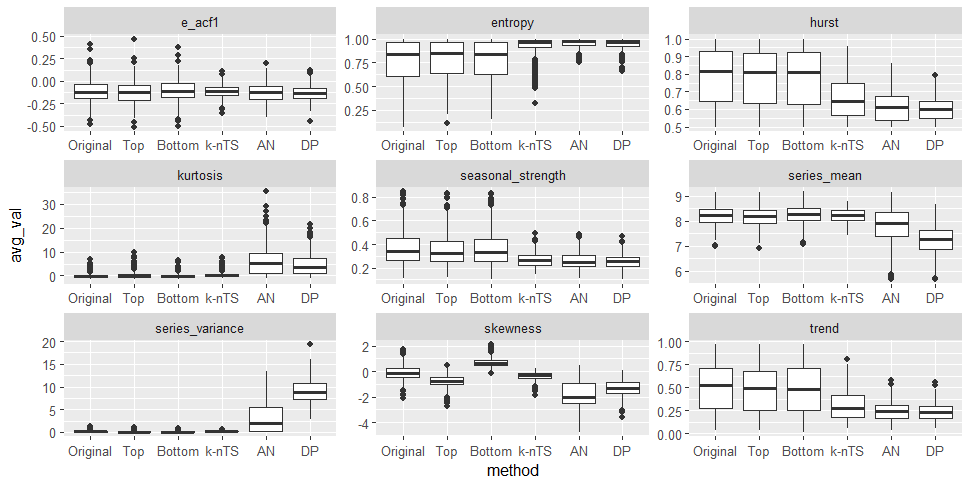
.

Letting denote the entropy of , the percentage difference between and is approximately

.

In **Figure 2**, we calculate the average feature value for each series across the protected datasets for each privacy method. We plot these distributions next to the distribution of each feature from the original data. **Table 2** contains the calculated between the distribution of each feature in the original data, and the distribution of the average protected feature values for each privacy method and feature.

**Figure 2**



**TABLE 2 (percentage differences between feature distributions)**

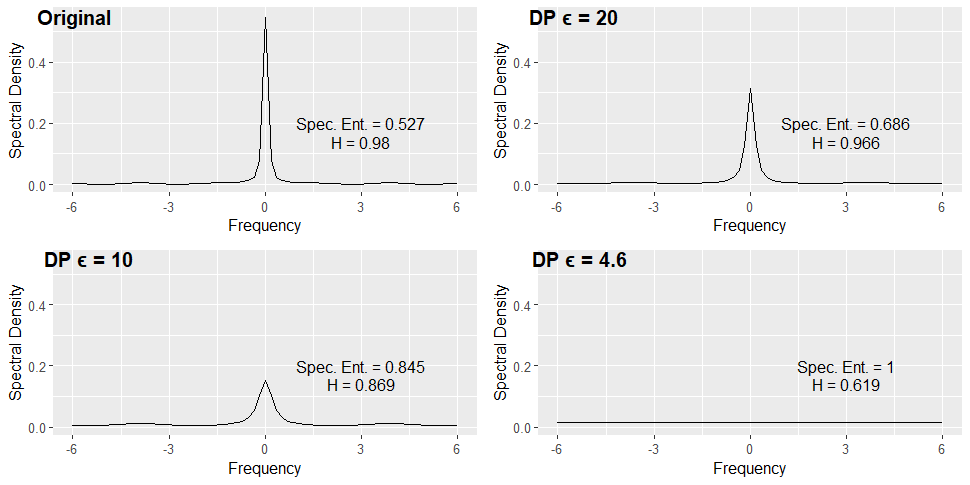
A screenshot of a computer

Description automatically generated with medium confidence

* Note that all of these results are on average across protected datasets.
* Top coding
  + Produces very small differences in most features. The most noticeable differences are in kurtosis, variance, and skewness.
    - 6.3% difference in kurtosis distribution, where the average kurtosis under top coding is 0.22 relative to 0.10 in the original data.
    - Top coding trims the upper quantiles of each series, and has produced a 1.3% difference in variance distribution, where values have decreased on average from 0.15 to 0.11, and a 14% difference in skewness distribution, where series now exhibit a left skew of -0.76 on average.
* Bottom coding
  + Produced less change in Kurtosis, but more change in variance and skewness.
  + The mechanism of change is the same – bottom coding trimmed the lower quantiles, reducing the average variance from 0.15 to 0.09 (larger change than top coding since the strongest skew values before were negative) and increasing the average skew to 0.69 (series are now right-skewed on average)
* K-nTS
  + The average e-acf value is approximately the same, but the distribution has less spread – difference of 3.78%
  + % changes in spectral entropy (8.9%) and Hurst (7.6%) indicate that series are more difficult to forecast (average spectral entropy increased from 0.76 to 0.92, Hurst decreased from 0.78 to 0.66).
  + 4% difference in kurtosis distribution, where the average increased from 0.1 to to 0.41, relative to the original data
  + Results in more left skew on average, (-0.39) but a smaller percentage difference in skew than top and bottom coding
  + Strength of trend and seasonality decreased on average to 0.31 and 0.27, respectively (were 0.5 and 0.37 in original data), consistent with lower Hurst coefficients and higher spectral entropies
  + K-nts produced minimal difference in the means of the series, and a slight increase in variance resulting in ~7% difference in variance distributions (the distribution of variance under k-nTS has less spread than the original distribution)
* AN/DP
  + Produced significant changes in every feature except e\_acf1
  + Entropy distributions differ by 14/17% (~1 for most series), Hurst distributions differ by 16/21%, (~.6 for most series)
  + Kurtosis and variance distributions differ by well over 100% - series have much higher variance and fatter tails
  + The mean distributions also differ by large percentages – we are looking at the log series, and random noise protection produces values that bias the mean downward, and produce left-skewed series
  + Strength of trend and seasonality have decreased on average to ~0.24 and ~0.26
* **Overall**
  + Top and bottom coding produce small changes in overall forecastability as estimated by the spectral entropy and Hurst coefficient 🡪 the randomness and long-term dependence of time series are relatively unaffected. These privacy methods do have significant effects on the distribution of time series values, namely the skewness, variance, and kurtosis.
  + K-nTS produces noticeable changes in forecastability 🡪 swapping values increases the randomness and reduces the long-term dependence of series, including reducing the strength of trend and seasonality. While variance is slightly higher on average under k-nTS, this method is relatively successful at preserving the means and skewness of series, especially relative to random noise protection. Overall, k-nTS makes the series more random, but preserves some of their distributional patterns.
  + AN/DP – random noise protection produces large changes in the distributions of time series, and significantly increases their randomness – spectral entropy and Hurst values predict poor forecast accuracy.
  + Rank privacy methods on average of average distributional difference (row-wise average of Table 2):
    - Top coding (2.35%)
    - Bottom coding (3.17%)
    - K-nTS (6.48%)
    - AN (80.04%)
    - DP (98.37%)

**Figure 3** shows an example of changes in the spectral density under increasing levels of differential privacy protection (decreasing values of ). The flattening of the spectral density reflects the addition of increasing amounts of random noise to the series, weakening and ultimately removing the original autocorrelations.

**FIGURE 3: Spectral densities for a single under different levels of differential privacy protection. Displays corresponding spectral entropy and hurst coefficient values.**



* 1. *Accuracy Results and Features*

**Table 3** contains the average MAE of one-step ahead point forecasts across all models and privacy parameters for each privacy method. More granular accuracy results are presented in the appendix. **Table 3** also contains the three privacy metrics from section 4.2, calculated using random samples of external data containing five confidential values from each time series. There is a clear relationship between forecast accuracy and the strength of privacy protection. While random noise protection provides the lowest risk of identification and attribute disclosure, the forecast error, on average, is nearly double under additive noise, and nearly triple under differential privacy. K-nTS provides a better trade-off, with significantly lower privacy risks than top- and bottom-coding, but improved accuracy over random noise protection.

**TABLE 3: average accuracy across forecasting models for each privacy method, and measures of identification and attribute disclosure risk for each privacy method.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **Privacy Method** | Original | Top Coding | Bottom Coding | k-nTS | Additive Noise | Differential Privacy |
| Average MAE | 685.85 | 708.62 | 747.80 | 1020.52 | 1250.14\* | 1981.74\* |
| IR (average identification prob) | - | 90% | 90% | 15% | 7% | 2% |
| IP (average proportion of correctly identified series) | - | 90% | 90% | 9% | 5% | 1% |
| AR (MAE of predicted attribute) | - | 100 | 100 | 1000 | 1500 | 2000 |

\* The average across models for additive noise and differential privacy excludes the VAR model error for AN (s = 1) and DP () as the errors in these cases were over 1000% larger than the error of any other model. The reasons for this will be explored in section -.

\* The highlighted results in this table are hypothetical, actual results will be computed once we finalize the privacy metrics.

**Table 4:** the rank of each model in terms of MAE and forecast error variance on the original data vs. the average rank across protected datasets. Rightmost column contains the average of the protected MAE and error variance ranks.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | MAE Ranks | | Forecast Error Variance Ranks | | Average Rank |
| Model | Original | Protected | Original | Protected | Protected |
| TES | 1 | 3.6 | 2 | 3.6 | 3.6 |
| ARIMA | 2 | 3.6 | 1 | 3.0 | 3.3 |
| RNN | 3 | 2.8 | 5 | 3.4 | 3.1 |
| DES | 4 | 3.2 | 3 | 2.4 | 2.8 |
| SES | 5 | 3.4 | 4 | 3.4 | 3.4 |
| LGBM | 6 | 4.4 | 7 | 5.4 | 4.9 |
| VAR | 7 | 7.0 | 6 | 6.8 | 6.9 |

In **Table 4,** the models are rank-ordered based on their MAE on the original data. We see that TES and ARIMA, which explicitly model the seasonality of the series, performed the best, consistent with the findings of the original M3 competition (Makridakis & Hibon, 2000). While our most complex model, the RNN, ranks third on the original data accuracy, it ranks first across the protected datasets. Furthermore, RNN, DES, and SES have higher ranks across the protected data than on the original data, and are the three most accurate models across the protected datasets, beating out ARIMA and TES. LGBM and VAR maintain the worst accuracy on the original and protected datasets.

The results for the error variance ranks are similar. ARIMA and TES have the lowest error variance on the original data. ARIMA is only outperformed by DES on protected error variance, TES is outperformed by three additional models: SES, DES, and RNN, all of which improve on their original rankings. LGBM and VAR maintain the highest error variance on the original and protected datasets. Overall, DES has the best average rank in terms of MAE and error variance, closely followed by RNN.

Similar to (Spiliotis et al. 2020), we assess the relationship between time series features and forecast accuracy using a multiple linear regression of the series-level MAE of model from each data set on the nine time series features and fixed effects for each privacy method parameter, where the fixed effect for the original data is included in the intercept. We perform a 1% trim for each variable to reduce the effect of outliers and take the log of the MAE as the dependent variable to address a large right-skew. All variables are then scaled to [0, 1] for comparability of the coefficients. We calculate models of the form,

**Table 5** contains the coefficient estimates for the regression for each forecasting model. The For each model is relatively low, ranging from For the machine learning models to

* Spectral entropy
  + statistically significant effect only for the machine learning models (the coefficients are similar in magnitude), where increased entropy increases forecast error.
* Hurst
  + Statistically significant effect on forecast accuracy (reduces accuracy) for SES, DES, and VAR
* Skewness/Kurtosis
  + Increased skewness/kurtosis have statistically significant effect of improving forecast accuracy for all models
  + Opposite result for skewness compared to (Spiliotis et al. 2020) who found skewness hurt accuracy in the m4 data
* Strength of Trend
  + Statistically significant improvement in forecast accuracy for SES, DES, VAR
  + There seems to be something going on with Hurst/Strength of trend and these three models
* Strength of Seasonality
  + Only statistically significant for TES – improves accuracy
* E\_acf1
  + Reduces accuracy for TES and ARIMA
  + Improves accuracy for machine learning models
* Mean/Variance
  + Increased values reduce forecast accuracy for all models – makes sense intuitively for variance, I am wondering if this is due to using MAE – maybe we should select a scale-independent error measure instead? Although this is consistent with higher mean being correlated with higher spectral entropy, which did not depend on any forecast accuracy.
* Fixed Effects
  + Several privacy method parameters show improvements in forecast accuracy across all most models – top 10%, bottom 20% and 40%, k-nTS with AN (s = 0.5), DP (
  + Each level of top and bottom coding seems to have a consistent effect across models.
  + SES, LGBM, and RNN are most robust to random noise protection – for AN (s = 1) these models do not have statistically significant reductions in accuracy, while the other models do – For AN (s = 1.5), these models actually show improved accuracy, and their accuracy under AN (s = 2) either does not have a statistically significant change (RNN) or is has a smaller reduction (SES, LGBM) than the other models.
  + For DP ( all models have large reductions in accuracy, but accuracy improves much more quickly for (LGBM, RNN) as increases.
  + For k-nTS, improves accuracy, whereas for there are almost no statistically significant effects. Only for exponential smoothing does k-nTS (k = 15) improve accuracy

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **SES** | **DES** | **TES** | **ARIMA** | **VAR** | **LGBM** | **RNN** |
| *Predictors* | *Estimates* | *Estimates* | *Estimates* | *Estimates* | *Estimates* | *Estimates* | *Estimates* |
| (Intercept) | 0.66 \*\*\* | 0.66 \*\*\* | 0.60 \*\*\* | 0.54 \*\*\* | 0.50 \*\*\* | 0.50 \*\*\* | 0.46 \*\*\* |
| Protection Parameter [Top\_0.1] | -0.15 \*\*\* | -0.14 \*\*\* | -0.15 \*\*\* | -0.14 \*\*\* | -0.11 \*\*\* | -0.14 \*\*\* | -0.14 \*\*\* |
| Protection Parameter [Top\_0.2] | 0.01 | 0.01 | 0.02 | 0.01 | 0.01 | 0.02 | 0.02 |
| Protection Parameter [Top\_0.4] | 0.03 \* | 0.02 | 0.04 \*\*\* | 0.03 \* | 0.03 \*\* | 0.03 \*\* | 0.05 \*\*\* |
| Protection Parameter [Bottom\_0.1] | 0.06 \*\*\* | 0.06 \*\*\* | 0.05 \*\*\* | 0.05 \*\*\* | 0.03 \*\* | 0.06 \*\*\* | 0.06 \*\*\* |
| Protection Parameter [Bottom\_0.2] | -0.38 \*\*\* | -0.38 \*\*\* | -0.38 \*\*\* | -0.38 \*\*\* | -0.31 \*\*\* | -0.38 \*\*\* | -0.41 \*\*\* |
| Protection Parameter [Bottom\_0.4] | -0.19 \*\*\* | -0.18 \*\*\* | -0.17 \*\*\* | -0.16 \*\*\* | -0.15 \*\*\* | -0.17 \*\*\* | -0.17 \*\*\* |
| Protection Parameter [knts\_5] | -0.00 | 0.00 | 0.02 | 0.02 | 0.01 | 0.02 \* | 0.01 |
| Protection Parameter [knts\_10] | -0.07 \*\*\* | -0.07 \*\*\* | -0.05 \*\*\* | -0.05 \*\*\* | -0.04 \*\*\* | -0.04 \*\*\* | -0.05 \*\*\* |
| Protection Parameter [knts\_15] | -0.03 \*\* | -0.03 \* | -0.02 \* | -0.01 | -0.01 | -0.01 | -0.01 |
| Protection Parameter [AN\_0.5] | -0.05 \*\*\* | -0.04 \*\*\* | -0.02 \* | -0.04 \*\* | -0.02 \* | -0.06 \*\*\* | -0.06 \*\*\* |
| Protection Parameter [AN\_1] | 0.01 | 0.04 \*\*\* | 0.07 \*\*\* | 0.04 \*\*\* | 0.05 \*\*\* | -0.00 | -0.01 |
| Protection Parameter [AN\_1.5] | -0.05 \*\*\* | -0.01 | 0.01 | -0.02 | 0.01 | -0.07 \*\*\* | -0.08 \*\*\* |
| Protection Parameter [AN\_2] | 0.08 \*\*\* | 0.11 \*\*\* | 0.13 \*\*\* | 0.09 \*\*\* | 0.10 \*\*\* | 0.03 \* | 0.01 |
| Protection Parameter [DP\_0.1] | 0.25 \*\*\* | 0.25 \*\*\* | 0.25 \*\*\* | 0.26 \*\*\* | 0.21 \*\*\* | 0.24 \*\*\* | 0.22 \*\*\* |
| Protection Parameter [DP\_1] | 0.21 \*\*\* | 0.22 \*\*\* | 0.22 \*\*\* | 0.22 \*\*\* | 0.18 \*\*\* | 0.08 \*\*\* | 0.07 \*\*\* |
| Protection Parameter [DP\_4.6] | 0.04 \*\*\* | 0.07 \*\*\* | 0.10 \*\*\* | 0.06 \*\*\* | 0.07 \*\*\* | 0.01 | -0.01 |
| Protection Parameter [DP\_10] | -0.02 | 0.01 | 0.02 | 0.01 | 0.02 | -0.01 | -0.02 \* |
| Protection Parameter [DP\_20] | -0.06 \*\*\* | -0.04 \*\*\* | -0.02 \* | -0.03 \* | -0.02 | -0.05 \*\*\* | -0.05 \*\*\* |
| entropy | 0.02 | -0.02 | 0.01 | 0.02 | 0.01 | 0.09 \*\*\* | 0.10 \*\*\* |
| hurst | 0.04 \* | 0.04 \* | 0.00 | -0.02 | 0.06 \*\*\* | 0.02 | 0.01 |
| skewness | -0.41 \*\*\* | -0.36 \*\*\* | -0.37 \*\*\* | -0.31 \*\*\* | -0.28 \*\*\* | -0.37 \*\*\* | -0.38 \*\*\* |
| kurtosis | -0.27 \*\*\* | -0.23 \*\*\* | -0.23 \*\*\* | -0.19 \*\*\* | -0.16 \*\*\* | -0.25 \*\*\* | -0.26 \*\*\* |
| trend | -0.09 \*\*\* | -0.11 \*\*\* | -0.03 | -0.01 | -0.10 \*\*\* | -0.00 | 0.01 |
| series mean | 0.30 \*\*\* | 0.28 \*\*\* | 0.29 \*\*\* | 0.32 \*\*\* | 0.22 \*\*\* | 0.39 \*\*\* | 0.43 \*\*\* |
| series variance | 0.60 \*\*\* | 0.59 \*\*\* | 0.58 \*\*\* | 0.61 \*\*\* | 0.45 \*\*\* | 0.65 \*\*\* | 0.71 \*\*\* |
| e acf1 | -0.00 | 0.02 | 0.02 \* | 0.03 \*\* | -0.01 | -0.02 \* | -0.03 \*\* |
| seasonal strength | 0.02 | 0.01 | -0.04 \*\*\* | -0.01 | 0.00 | 0.00 | 0.00 |
| Observations | 7692 | 7691 | 7699 | 7697 | 7689 | 7702 | 7702 |
| R2 / R2 adjusted | 0.249 / 0.246 | 0.242 / 0.239 | 0.265 / 0.263 | 0.245 / 0.242 | 0.248 / 0.246 | 0.197 / 0.194 | 0.195 / 0.192 |
| *\* p<0.05   \*\* p<0.01   \*\*\* p<0.001* | | | | | | | |

1. **Conclusions**

**References**

Abowd, J. M., Gittings, K., McKinney, K. L., Stephens, B. E., Vilhuber, L., & Woodcock, S. (2012). *Dynamically consistent noise infusion and partially synthetic data as confidentiality protection measures for related time-series*. 41.

Bandara, K., Bergmeir, C., & Smyl, S. (2018). Forecasting Across Time Series Databases using Recurrent Neural Networks on Groups of Similar Series: A Clustering Approach. *ArXiv:1710.03222 [Cs, Econ, Stat]*. http://arxiv.org/abs/1710.03222

Boone, T., Ganeshan, R., Jain, A., & Sanders, N. R. (2019). Forecasting sales in the supply chain: Consumer analytics in the big data era. *International Journal of Forecasting*, *35*(1), 170–180. https://doi.org/10.1016/j.ijforecast.2018.09.003

Chen, C., & Liu, L.-M. (1993). Forecasting time series with outliers. *Journal of Forecasting*, *12*(1), 13–35. https://doi.org/10.1002/for.3980120103

Crimi, N., & Eddy, W. (2014). Top-Coding and Public Use Microdata Samples from the U.S. Census Bureau. *Journal of Privacy and Confidentiality*, *6*(2). https://doi.org/10.29012/jpc.v6i2.639

Davydenko, A., & Fildes, R. (2013). Measuring forecasting accuracy: The case of judgmental adjustments to SKU-level demand forecasts. *International Journal of Forecasting*, *29*(3), 510–522. https://doi.org/10.1016/j.ijforecast.2012.09.002

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, *3*(1), 1376. https://doi.org/10.1038/srep01376

Fildes, R., Goodwin, P., Lawrence, M., & Nikolopoulos, K. (2009). Effective forecasting and judgmental adjustments: An empirical evaluation and strategies for improvement in supply-chain planning. *International Journal of Forecasting*, *25*(1), 3–23. https://doi.org/10.1016/j.ijforecast.2008.11.010

Fildes, R., Goodwin, P., & Önkal, D. (2019). Use and misuse of information in supply chain forecasting of promotion effects. *International Journal of Forecasting*, *35*(1), 144–156. https://doi.org/10.1016/j.ijforecast.2017.12.006

Fulcher, B. D., & Jones, N. S. (2014). Highly Comparative Feature-Based Time-Series Classification. *IEEE Transactions on Knowledge and Data Engineering*, *26*(12), 3026–3037. https://doi.org/10.1109/TKDE.2014.2316504

Goerg, G. M. (n.d.). *Forecastable Component Analysis*. 9.

Goldfarb, A., & Tucker, C. (n.d.). *Why Managing Consumer Privacy Can Be an Opportunity*. 6.

Goldfarb, A., & Tucker, C. E. (2011). Privacy Regulation and Online Advertising. *Management Science*, *57*(1), 57–71. https://doi.org/10.1287/mnsc.1100.1246

Gonçalves, C., Bessa, R. J., & Pinson, P. (2021). A critical overview of privacy-preserving approaches for collaborative forecasting. *International Journal of Forecasting*, *37*(1), 322–342. https://doi.org/10.1016/j.ijforecast.2020.06.003

Goncalves, C., Bessa, R. J., & Pinson, P. (2021). Privacy-Preserving Distributed Learning for Renewable Energy Forecasting. *IEEE Transactions on Sustainable Energy*, *12*(3), 1777–1787. https://doi.org/10.1109/TSTE.2021.3065117

Goncalves, C., Pinson, P., & Bessa, R. J. (2021). Towards Data Markets in Renewable Energy Forecasting. *IEEE Transactions on Sustainable Energy*, *12*(1), 533–542. https://doi.org/10.1109/TSTE.2020.3009615

Hewamalage, H., Bergmeir, C., & Bandara, K. (2021). Recurrent Neural Networks for Time Series Forecasting: Current status and future directions. *International Journal of Forecasting*, *37*(1), 388–427. https://doi.org/10.1016/j.ijforecast.2020.06.008

Hewamalage, H., Bergmeir, C., & Bandara, K. (2022). Global models for time series forecasting: A Simulation study. *Pattern Recognition*, *124*, 108441. https://doi.org/10.1016/j.patcog.2021.108441

Imtiaz, S., Horchidan, S.-F., Abbas, Z., Arsalan, M., Chaudhry, H. N., & Vlassov, V. (2020). Privacy Preserving Time-Series Forecasting of User Health Data Streams. *2020 IEEE International Conference on Big Data (Big Data)*, 3428–3437. https://doi.org/10.1109/BigData50022.2020.9378186

Kang, Y., Hyndman, R. J., & Smith-Miles, K. (2017). Visualising forecasting algorithm performance using time series instance spaces. *International Journal of Forecasting*, *33*(2), 345–358. https://doi.org/10.1016/j.ijforecast.2016.09.004

Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., Ye, Q., & Liu, T.-Y. (n.d.). *LightGBM: A Highly Efficient Gradient Boosting Decision Tree*. 9.

Khosrowabadi, N., Hoberg, K., & Imdahl, C. (2022). Evaluating human behaviour in response to AI recommendations for judgemental forecasting. *European Journal of Operational Research*, *303*(3), 1151–1167. https://doi.org/10.1016/j.ejor.2022.03.017

Koning, A. J., Franses, P. H., Hibon, M., & Stekler, H. O. (2005). The M3 competition: Statistical tests of the results. *International Journal of Forecasting*, *21*(3), 397–409. https://doi.org/10.1016/j.ijforecast.2004.10.003

Li, L., Kang, Y., & Li, F. (2022). Bayesian forecast combination using time-varying features. *International Journal of Forecasting*, S0169207022000930. https://doi.org/10.1016/j.ijforecast.2022.06.002

Liyue Fan & Li Xiong. (2014). An Adaptive Approach to Real-Time Aggregate Monitoring With Differential Privacy. *IEEE Transactions on Knowledge and Data Engineering*, *26*(9), 2094–2106. https://doi.org/10.1109/TKDE.2013.96

Luo, J., Hong, T., & Fang, S.-C. (2018). Benchmarking robustness of load forecasting models under data integrity attacks. *International Journal of Forecasting*, *34*(1), 89–104. https://doi.org/10.1016/j.ijforecast.2017.08.004

Makridakis, S., & Hibon, M. (2000). The M3-Competition: Results, conclusions and implications. *International Journal of Forecasting*, *16*(4), 451–476. https://doi.org/10.1016/S0169-2070(00)00057-1

Makridakis, S., Spiliotis, E., & Assimakopoulos, V. (2018). The M4 Competition: Results, findings, conclusion and way forward. *International Journal of Forecasting*, *34*(4), 802–808. https://doi.org/10.1016/j.ijforecast.2018.06.001

Makridakis, S., Spiliotis, E., & Assimakopoulos, V. (2022). M5 accuracy competition: Results, findings, and conclusions. *International Journal of Forecasting*, S0169207021001874. https://doi.org/10.1016/j.ijforecast.2021.11.013

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Nicholson, W. B., Matteson, D. S., & Bien, J. (2017). VARX-L: Structured regularization for large vector autoregressions with exogenous variables. *International Journal of Forecasting*, *33*(3), 627–651. https://doi.org/10.1016/j.ijforecast.2017.01.003

Nin, J., & Torra, V. (2009). Towards the evaluation of time series protection methods. *Information Sciences*, *179*(11), 1663–1677. https://doi.org/10.1016/j.ins.2009.01.024

Petropoulos, F., Apiletti, D., Assimakopoulos, V., Babai, M. Z., Barrow, D. K., Taieb, S. B., Bergmeir, C., Bessa, R. J., Bijak, J., Boylan, J. E., Browell, J., Carnevale, C., Castle, J. L., Cirillo, P., Clements, M. P., Cordeiro, C., Oliveira, F. L. C., Baets, S. D., Dokumentov, A., … Ziel, F. (2022). *Forecasting: Theory and practice*. 167.

Petropoulos, F., & Siemsen, E. (2022). Forecast Selection and Representativeness. *Management Science*, mnsc.2022.4485. https://doi.org/10.1287/mnsc.2022.4485

Qi, L., Li, X., Wang, Q., & Jia, S. (2022). fETSmcs: Feature-based ETS model component selection. *International Journal of Forecasting*, S0169207022000954. https://doi.org/10.1016/j.ijforecast.2022.06.004

Rose, O. (n.d.). *Estimation of the Hurst Parameter of Long-Range Dependent Time Series*. 16.

Smyl, S. (2020). A hybrid method of exponential smoothing and recurrent neural networks for time series forecasting. *International Journal of Forecasting*, *36*(1), 75–85. https://doi.org/10.1016/j.ijforecast.2019.03.017

Sobolev, D. (2017). The effect of price volatility on judgmental forecasts: The correlated response model. *International Journal of Forecasting*, *33*(3), 605–617. https://doi.org/10.1016/j.ijforecast.2017.01.009

Sommer, B., Pinson, P., Messner, J. W., & Obst, D. (2021). Online distributed learning in wind power forecasting. *International Journal of Forecasting*, *37*(1), 205–223. https://doi.org/10.1016/j.ijforecast.2020.04.004

Spiliotis, E., Kouloumos, A., Assimakopoulos, V., & Makridakis, S. (2020). Are forecasting competitions data representative of the reality? *International Journal of Forecasting*, *36*(1), 37–53. https://doi.org/10.1016/j.ijforecast.2018.12.007

Sweeney, L. (2002). k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 557–570. https://doi.org/10.1142/S0218488502001648

Talagala, T. S., Li, F., & Kang, Y. (2022). FFORMPP: Feature-based forecast model performance prediction. *International Journal of Forecasting*, *38*(3), 920–943. https://doi.org/10.1016/j.ijforecast.2021.07.002

Véliz, C., & Grunewald, P. (2018). Protecting data privacy is key to a smart energy future. *Nature Energy*, *3*(9), 702–704. https://doi.org/10.1038/s41560-018-0203-3

Wang, X., Smith, K., & Hyndman, R. (2006). Characteristic-Based Clustering for Time Series Data. *Data Mining and Knowledge Discovery*, *13*(3), 335–364. https://doi.org/10.1007/s10618-005-0039-x

Willinger, W., Paxson, V., Taqqu, M. S., & Willinger, W. (n.d.). *Self-Similarity and Heavy Tails: Structural Modeling of Network Tra c*. 26.

1. For examples in the United States, see [this](https://iapp.org/resources/article/us-state-privacy-legislation-tracker/) map. [↑](#footnote-ref-1)
2. See the description of anonymous information given in [Recital 26](https://gdpr-info.eu/recitals/no-26/) of the GDPR. [↑](#footnote-ref-2)
3. See articles 6, 45, and 46 of the GDPR. [↑](#footnote-ref-3)
4. See the [Gramm-Leach-Bliley act](https://www.govinfo.gov/app/details/PLAW-106publ102). [↑](#footnote-ref-4)
5. See [several python libraries](https://www.infoq.com/news/2022/02/differential-privacy-python/) including PipelineDP and PyDP. [↑](#footnote-ref-5)
6. See the [OpenDP project](https://cloudblogs.microsoft.com/opensource/2020/05/19/new-differential-privacy-platform-microsoft-harvard-opendp/). [↑](#footnote-ref-6)
7. See [descriptions](https://www.apple.com/privacy/features/) of Apple's privacy features. [↑](#footnote-ref-7)