Sentence - 1:

1. However, the existing placement strategies do not care users' privacy which is a compelling but less studied problem that needs to be addressed.
2. Considering the users' privacy and limited resources of mobile devices, it is impossible to deploy all services on the edge clouds.
3. Our algorithm could not only protect users' privacy but also meet users' service demands through mobile edge clouds.

Sentence - 2:

1. Data mining has **heralded** the major breakthrough in data analysis, serving as a "super cruncher" to discover hidden information and valuable knowledge in big data systems.
2. A malicious participant may **tamper with** the information gain by providing a low quality data.
3. The collection of big data usually involves various parties who are interested in **pooling their private** data sets together to jointly train machine-learning models that yield more accurate prediction results.
4. The result demonstrate that our system can provide a strong privacy protection for individual data owner **while maintaining the prediction accuracy of the original trained model.**
5. Our experimental evaluations verify that our system can provide strong privacy protection while achieving a high prediction accuracy comparable to the original GBDT model.
6. White-box model is ideal for decision trees, but may cause private information leakage.
7. Figure one presents an overview of our system, where multiple data owners agree on sharing data set to extract common knowledge, but do not want to reveal any private information about their own data.
8. Though we expect all participants to be equally capable to train a tree with the same effectiveness, it is obviously impractical in real world.

Sentence - 3:

1. So however richer he was in the past days, he is a loser now.
2. Hence, if we want to model the small distances accurately in the map, most of the points that are at a moderate distance from datapoint i will have to be placed much too far away in the two-dimensional map.

Sentence - 4:

1. Many data mining algorithm have been developed that harness differential privacy
2. How exactly we go about protecting the privacy of individuals while also building the models and discovering knowledge is a large question, and one that this paper weighs in on.

3. Note that our aim is not to beat these non-private techniques (which is almost impossible), but simply use them as a reference point for how high prediction accuracy can realistically get for the dataset we have.

Sentence - 5:

1. This motivate us to investigate the distributed the distributed privacy-preserving DA against the dishonest nodes in network systems.
2. The initial state usually denotes each node's sensitive information (e.g., age, location, income, etc.). But the aggregated data only reflects the statistics of all nodes' state (e.g., their average, sum, variance), which will not jeopardize the privacy of each individual node directly if the number of nodes in the network is **sufficiently large**.
3. To tackle this dilemma, federated learning was proposed to train a collaborative model with privacy-preserving algorithms while keeping private data locally.