Paper Review #3:
Differential Privacy in Practice: Expose Your Epsilons!

Summary 1: Differential Privacy in Practice: Expose Your Epsilons! discusses the importance of epsilons in differential privacy. Epsilons are an essential part of differential privacy as they decide how private a database is. However, there is a lack of consensus and understanding on how to calculate the best epsilon for databases. The paper suggests creating the Epsilon Registry which keeps track of database epsilons so that there could be a better understanding of them.

Summary 2: Differential Privacy in Practice: Expose Your Epsilons! discusses the lack of understanding of an important element in differential privacy. Differential privacy keeps information about people private using a value called epsilon. However, the paper found that epsilon is not understand very well and needs to be researched further. So the paper suggests an Epsilon Registry that holds database epsilons so that more can be learned about them.

Question and Answer
What is the problem?

- There is very little understanding on how to find the best epsilon for any database. Also, between differential privacy experts, there was no consensus on how to make epsilon or approach making epsilon.

Why is it interesting and important?

- Differential privacy allows users to learn important information without learning private information. Choosing the correct epsilon is important for ensuring that a database is private and usable.

Why is it hard?

- There is a lack of certainty for what is the optimal degree of privacy lost or a formula to calculate epsilon efficiently.

Why hasn’t it been solved before?

- There is no shared source between the differential privacy community to learn from. Creating a lack of shared understand for how epsilon should be created.

What are the key components of the proposed approach and results?

- A key component of the research is the case studies that are conducted about the methodologies experts use to calculate epsilon.

Paper Review #3:
How Much Is Enough? Choosing Epsilon for Differential Privacy

Summary 1: How Much Is Enough? Choosing Epsilon for Differential Privacy discusses a glaring problem in differential privacy. Most literature on the topic focus on its theoretical implementations but not on applying it in practice. Therefore, choosing the right value of epsilon, an essential part of differential privacy, is often overlooked. As epsilon is what decides how private the database is.

Summary 2: How Much Is Enough? Choosing Epsilon for Differential Privacy talks about a problem in differential privacy that's often overlooked. Differential privacy helps to keep information private using a value called epsilon. However, people often overlook how to choose the correct epsilon to ensure privacy.

Question and Answer

What is the problem?

- The problem is that differential privacy isn't discussed much on applying it in practice. Therefore, selecting an appropriate epsilon is difficult and the epsilon does not always correlate to a practical privacy standard.

Why is it interesting and important?

- For differential privacy, choosing an appropriate epsilon is essential for balancing utility and privacy for a dataset.

Why is it hard?

- The process for choosing an appropriate epsilon is never the same for two different databases as you must consider all the information relevant to the databases to ensure that the data is private but also usable.

Why hasn't it been solved before?

- A lot of literature focus on the implementation of differential privacy but doesn't focus on ensuring that privacy is kept on the system. The value of epsilon is the responsibility of the users, which isn't ideal.

What are the key components of the proposed approach and results?

- One key component of the approach is creating upper bounds for the adversary's probability of getting a correct guess. The component shows how the smaller an epsilon is, the smaller the probability for the adversary making the correct guess.