Paper Review #4:
Differential Privacy Under Fire

Summary 1: Differential Privacy Under Fire discusses the privacy vulnerabilities of systems that promise differential privacy by processing user queries, such as PINQ. These systems make it easier for data curators to create differentially private databases. The paper mentions the main attacks these systems are vulnerable to, but also provides a programming language (FIZZ) that is effective against the vulnerabilities.

Summary 2: Differential Privacy Under Fire talks about how systems that promise to make databases private have certain vulnerabilities. These vulnerabilities undermine the privacy guarantees of the system as they allow attackers to learn sensitive information. The paper provides a solution called FIZZ, which allows these systems to be protected against those attacks.

Question and Answer

What is the problem?

- Systems that process user queries and apply differential privacy, such as PINQ, are vulnerable to convert-channel attacks. These attacks include timing attacks, state attacks, and privacy budget attacks.

Why is it interesting and important?

- Systems like PINQ make it easier to make a database differentially private but they cannot be used until all the vulnerabilities are patched. By solving the problems these systems face, having differentially private databases can be more widely spread.

Why is it hard?

- These systems focused on the idea that the querier could only get information from the query result. However, some of these attacks focus on how the query is ran such as time attacks which can glean sensitive information by timing how long the query takes to run.

Why hasn’t it been solved before?

- These systems, along with differential privacy, are new and haven’t been put under enough scrutiny to be complete. There needs to be more research done until the systems can run without releasing private information.

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

- A key component of the research are the case studies for PINQ and Airvat that reveal their vulnerabilities. As well as the proof-of-concept of their programming language FUZZ, demonstrating a potential solution to the problem.

Paper Review #4:
Visualizing Privacy-Utility Trade-Offs in Differentially Private Data Releases

Summary 1: Visualizing Privacy-Utility Trade-Offs in Differentially Private Data Releases discusses how there is little understanding on how to choose the best epsilon to make a database differentially private. The solution provided is a system called Visualizing Privacy (ViP) which shows users how different epsilons affect the output of the data. It allowed people with little knowledge of differential privacy to understand how epsilons effected the data.

Summary 2: Visualizing Privacy-Utility Trade-Offs in Differentially Private Data Releases talks about how an essential part of differential privacy isn't well understood. However, the research provides a system called Visualizing Privacy (ViP) that can help users understand it better. It visualizes the effects of the mechanism so that people with little understanding of differential privacy can make better judgements about it.

Question and Answer
What is the problem?

- There is little guidance on how to choose the right epsilon for a database that provides appropriate privacy and utility.

Why is it interesting and important?

- Choosing the right epsilon is essential for balancing utility and privacy for a dataset. ViP allows database curators to make better decisions by understanding how different epsilons affect the release of the data.

Why is it hard?

- There is no agreed upon way to create an epsilon among differential private experts, especially for databases that have require different levels of privacy. Also, many data curators aren't experts in differential privacy, making the challenge of selecting the best epsilon even more difficult.

Why hasn't it been solved before?

- Differential privacy is still a relatively new field and the lack of consensus between experts make it difficult for a formula for epsilon to be created. Additionally, the there is a low understanding of differential privacy among the general population so implementing it can be confusing for people to understand what it's doing.

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

- A key component of the research is the establishment of ViP as it's a helpful tool for understanding and deciding an appropriate epsilon. Additionally, the results of people with little knowledge of differential privacy answering questions after using ViP proved that ViP is useful.