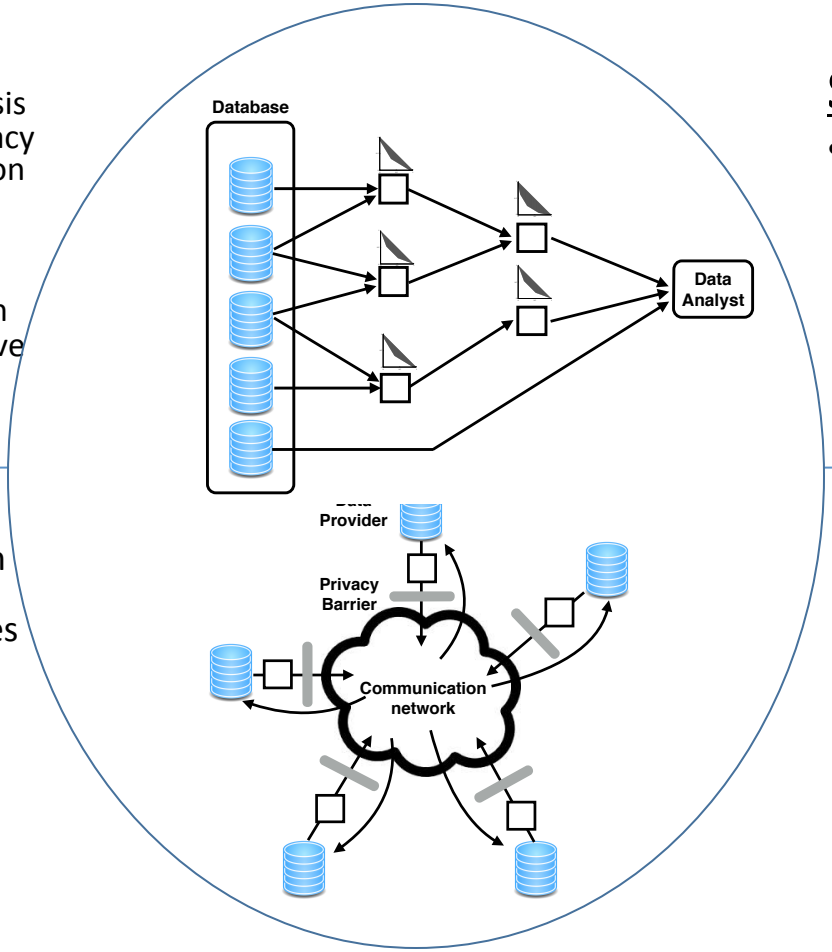
Fundamental Limits in Differential Privacy

Challenge:

- Macroscopic analysis analysis of privacy: how does privacy degrade under composition of many interacting components?
- Microscopic analysis of privacy: how do we design each component to achieve optimal utility-privacy tradeoff?



Solution:

- Operational interpretation of differential privacy as hypothesis testing provides a new perspective as *privacy region*
- The region perspective provides a new tool for designing dominant mechanisms

Award 1527754
PI: Sewoong Oh

Scientific Impact:

- Develop privacy calculus, a computational tool for analyzing how privacy preserving data processing components interact.

Broader Impact:

- The proposal has a potential to establish alternative privacy models and make privacy accessible to uninitiated users by developing privacy calculus.