# Differential Privacy (Weaker notion)

$X$: The data universe.

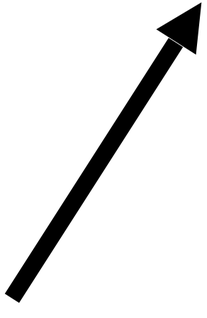
$D \subset X$: The dataset (one element per person)

Definition: An algorithm $M$ is $(\epsilon, \delta)$-differentially private if for all pairs of neighboring datasets $D$, $D'$, and for all outputs x:

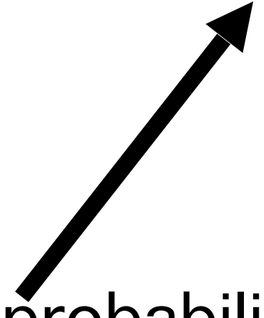
$$\Pr\left[M(D) = x\right] \leq \exp(\epsilon) * \Pr\left[M(D') = x\right] + \delta$$

35

Quantifies information leakage



Allows for a small probability of failure



# Differential Privacy (Weaker notion)

$X$: The data universe.

$D \subset X$: The dataset (one element per person)

Definition: An algorithm $M$ is $(\epsilon, \delta)$-differentially private if for all pairs of neighboring datasets $D$, $D'$, and for all outputs x:

$$\Pr\left[M(D) = x\right] \leq \exp(\epsilon) * \Pr\left[M(D') = x\right] + \delta$$

Quantifies information leakage

Allows for a small probability of failure

# Some useful properties for ML