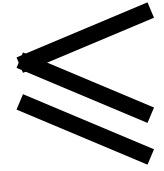
A randomized computation M is **differentially private** if there exists a value *epsilon* such that:

for any possible input dataset A,
for any possible input record r,
for any possible outcome S,

$$\Pr[M(A) = S] \quad \exp(\text{epsilon}) \times \Pr[M(A \pm r) = S].$$




Computations provide privacy.


Much “for any”. Covers all contexts, secrets, concerns.

Think “1 + epsilon” for epsilon much less than 1.

**Operational: directly covers participation concerns.**

A randomized computation M is **differentially private** if there exists a value *epsilon* such that:

for any possible input dataset A,
for any possible input record r,
for any possible outcome S,

$$\Pr[M(A) = S] \leqslant \exp(\text{epsilon}) \times \Pr[M(A \pm r) = S].$$

differential privacy,

but at what cost?