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]     exp(epsilon) x Pr[M(A ± 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,<br>
for any possible input record r,<br>
for any possible outcome S,

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

# differential privacy,
# but at what cost?