




Outline:

- consider 4 distinct concepts of democracy
- first three Flawed
- #4: good (DP)

Privacy Concept #1: "Anonymization"

- basic idea: take a sensitive dataset / DB, and modify it in order to protect privacy/identity, while hopefully still being useful.
- two operations:
 - redaction/deleting an entire column
 - Coarsening: Reducing resolution of cols.

One possible goal:

K-anonymization

Fatal flaw = Reverse engineering via
combining K-anon DBs
+ other info.

Concept #2: Aggregation

Ex: Computing the average
of a set of numbers.

e.g. $x_1, x_2, x_3 \dots x_n \in \mathbb{R}$

representing the salaries
of employees.

(a) $\bar{x} = \frac{1}{n} \sum x_i \rightarrow \$47,319.32$

$b = \frac{1}{n+1} \sum x_i$

so $(n+1)b - n\bar{x} = x_{n+1}$

$\bar{x} + [\bar{x}/\sqrt{n}, \bar{x}/\sqrt{n}]$

