• anonymity (e.g., K-anom.)
• aggregation
• "no harm"
• DP: no harm to you specifically due to your data

D vs. D'

algo

output 0 0

D
Randomized Response

- embarrassing questions:
  "Have you ever shoplifted?"
  "Do you believe in alien abductions?"

RR:

- answer truthfully
  - flip coin
  - flip again
  - if heads, "yes"; tails, "no"

- flip dice
  - if 1, 2, 3, 4, "yes"; 5, 6, "no"
Utility/accuracy analyses

• population of size n all follow this RR

• use $\{x_h, n\}$ as underlying true answers & $\{y_t, n\}$ as responses to RR

• $t = \text{fraction of pop with } H \Rightarrow \frac{m}{n} = y$

\[
\Pr["y_t" | y] = \left(\frac{1}{2}\right) \cdot 1 + \left(\frac{1}{2}\right) \left(\frac{1}{2}\right) \\
= \frac{1}{2} + \frac{1}{4} = \frac{3}{4}
\]

\[
\Pr["y_t" | y] = \left(\frac{1}{2}\right) \cdot 0 + \left(\frac{1}{2}\right) \left(\frac{1}{2}\right) \\
= \frac{1}{4}
\]
Pr \left[ y' \right] = t \left( \frac{3}{4} \right) + (1-t) \left( \frac{1}{4} \right) \\
= \frac{1}{4} + \frac{3}{2}

Pr \left[ y' \right] = 9

q = \frac{1}{t} + \frac{1}{2} \quad \text{solve for } t

\hat{q} = \text{estimation of } q \\
\text{from running each of } n \text{ times}

\text{Fact. With very high prob.}

1 \hat{q} - q \leq \frac{1}{\sqrt{n}} \Rightarrow 1 \hat{q} - q \to 0

t \pm \frac{1}{\sqrt{n}}
Definition of DP

We say that an algorithm $A$ satisfies $\varepsilon$-DP if for any pair of neighboring inputs $D$ and $D'$, if

$$\Pr[\text{output space}]$$

$D$ and $D'$ are randomized, then $\Pr[A \gets D] \leq \exp(\varepsilon) \Pr[A \gets D']$. 

Please note that the diagram is not fully legible due to handwriting and the nature of the drawing. It seems to depict the relationship between $A$ and the input spaces $D$ and $D'$, along with the randomized output space.
Formally:
- Let $A(D), A(D')$ denote the random output of $A$ under $D, D'$.
We want that for any subset $S$ of the output space of $A$,

$$\Pr[A(D) \in S] \leq e^{-\epsilon \Pr[A(D') \in S]}.$$