Differential Privacy

Alice	P
Bob	P
Charlie	P
Dave	P
Eve	F
Fred	P
Gina	F

ESTR 2018 Grades

Statistics
1. How many passed?
2. Did Dave pass? private
3. How many girls passed? grey area...

Private Information

1. Anonymize. This could work in some cases.

Name	Weight	Smoker
Bob	57kg	Yes

side-info → "How many 57kg heavy smokers are there?" → can still infer some info from this.

Doesn't work in general

2. Set up rules: e.g. in total 100 students, only answer queries that concern 50 or more students.

Still has problems.

Ask 2 questions: "How many passed?"
"How many not named Dave passed?" ✓ ✗

③ "Lie" a little bit (:-)

Eg. 100 students, 85 passed.

"How many passed?"

"How many ≠Dave passed?"

True	My answer
85	88
84	82

How to "lie"?

A mechanism is a probabilistic algorithm for answering queries.

On every question, lie independently.

		Fake ans
Alice	P	P
Bob	P	P
Charlie	P	F
Dave	P	P
Eve	F	P
Fred	P	P
Gina	F	F
# Passes = a		$\hat{A}$
true ans		r.v.

Flip a coin with prob. p, change a grade

Say $p=0.2$,

Let M be the answer now which is a r.v.

$$E[\hat{A}] = (1-p)a + p(n-a)$$
$$= (1-2p)a + pn$$

We want $E[M] = a$.

$\Rightarrow$ M outputs $\dfrac{\hat{A} - pn}{1-2p}$

Utility ≡≡≡ Privacy

Typical difference

$\rightarrow E[(M-a)^2] = Var[M]$

$\rightarrow$ So let $U(M) = \dfrac{1}{SD(M)} = \dfrac{1}{\sqrt{Var[M]}}$

If $M=a$, w.p. 1, $Var[M]=0$, $U(M)\to\infty$, but no privacy.

Privacy.

You have some beliefs about the grades. $P_1, P_2, \cdots, P_n$. e.g., $P(P_{Alice}=1 \text{ AND } P_{Bob}=0) = 0.2$.

knowing info from M should not change my belief, otherwise it's leaking information.

So, $P(P_{Dave}=1 \mid M=m, P_{-Dave}=p) = P(P_{Dave}=1 \mid P_{-Dave}=p)$

But this is not quite right.
(nothing can change your "prejudice")

P_{-Dave} : grades for all other students.
This should hold for all students $\Rightarrow$
M is independent of the true answers

$\frac{1}{\varepsilon}$ - Differential Privacy:

For $\forall$ two databases that differ in 1 row
for every m,

$$e^{-\varepsilon} \le \frac{P(M=m)}{P(M'=m)} \le e^{\varepsilon}, \quad \varepsilon \to 0.$$

$e^{\pm\varepsilon}$

This means:

$$P(P_{Dave}=1 \mid M=m, P_{-Dave}=p) = \frac{P(M=m \mid P_D=1, -)\, P(P_D=1 \mid -)}{P(M=m \mid -)}$$

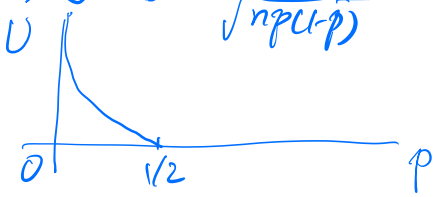
change by at most $e^{\pm\varepsilon}$, $\approx 1 \pm \varepsilon$.

Utility of M. $\frac{1}{\delta(M)}$

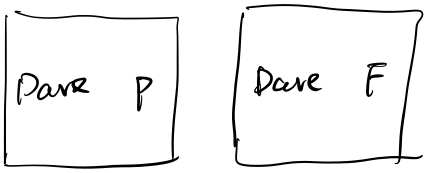
$\frac{\hat{A} - pn}{1-2p}$ $\hat{A}$: flip each row w.p. p.

$Var[\hat{A}] = Var[Binomial(n,p)] = np(1-p)$

$\Rightarrow \delta(M) = \frac{\sqrt{np(1-p)}}{1-2p}$ $\Rightarrow U(M) = \frac{1-2p}{\sqrt{np(1-p)}}$



Privacy of M : $\frac{1}{\varepsilon}$



$\frac{P(outcome)}{P(outcome')} = \frac{p}{1-p}$ or $\frac{1-p}{p}$

$\in e^{\pm\varepsilon}$ where

$\varepsilon = \ln \frac{1-p}{p}$