Performance Metric

- Accuracy (top-1, top-10 error, precision, recall, etc.)
- Training time
- Memory
- Test time
- Robustness
- Privacy
- Fairness
- Interpretability
The Netflix Challenge

<table>
<thead>
<tr>
<th>User</th>
<th>Inside Out</th>
<th>Good Will Hunting</th>
<th>Mean Girls</th>
<th>Terminator</th>
<th>Titanic</th>
<th>Warrior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tina Fey</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>?</td>
<td>1</td>
</tr>
<tr>
<td>Helen Mirren</td>
<td>2</td>
<td>?</td>
<td>?</td>
<td>2</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Sylvester Stallone</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Tom Hanks</td>
<td>?</td>
<td>3</td>
<td>1</td>
<td>?</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>George Clooney</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

<user, movie, date of rating, rating>

~1M ratings, .5M users, 20k movies
$1M

P=NP?
Can you imagine being so angry at #BobMurray you write ‘Eat Shit Bob’ on your bonus cheque, only to have #JohnOliver turn it into a song? Fucking legendary.

Do you share voter information with other agencies or groups?

Yes. Elections Canada shares voter information from the National Register of Electors with all provincial and territorial electoral agencies and with some municipalities for election purposes only. Sharing voter registration information improves the accuracy of voters lists, making it easier to vote. It also reduces duplication, saving taxpayer money.

As required by the Canada Elections Act, we also provide voters lists (containing name, address and unique identifier number) to candidates, members of Parliament and registered and eligible political parties, who may use the information for specific, authorized purposes. Refer to the Guidelines for Use of the Lists of Electors to learn more.

Note that we do not share voter information with any other organizations, including social media platforms and media.
Anonymization is not enough

The 1997 voting list for Cambridge, Massachusetts, contains demographics on 54,805 voters. Of these, birth date, which contains the month, day, and year of birth, alone can uniquely identify the name and address of 12 percent of the voters. One can identify 29 percent of the list by just birth date and gender, 69 percent with only a birth date and a 5-digit ZIP code, and 97 percent (53,033 vot-

<table>
<thead>
<tr>
<th>ZIP Code</th>
<th>Birth Date</th>
<th>Gender</th>
<th>Race</th>
</tr>
</thead>
<tbody>
<tr>
<td>33171</td>
<td>7/15/71</td>
<td>m</td>
<td>Caucasian</td>
</tr>
<tr>
<td>02657</td>
<td>2/18/73</td>
<td>f</td>
<td>Black</td>
</tr>
<tr>
<td>20612</td>
<td>3/12/75</td>
<td>m</td>
<td>Asian</td>
</tr>
</tbody>
</table>

Table 2. Deidentified Data that Are Not Anonymous.

Table 3. Uniqueness of Demographic Fields in Cambridge, Massachusetts, Voter List.

Differencing Attack

• Restrict queries to be “large”
• “How many people have disease X?”
• “How many people, not named YYL, have disease X?”
• Can design sequence of queries to avoid detection
Sacrifice “just a few”
Maybe just refuse to give any info?
Randomization is KEY

• Deterministic query $q$ on database $D$

• Suppose $q$ is non-constant

• Exist nearby $D_1$ and $D_2$ such that applying $q$ on one of them reveals the difference
Bounded noise if NOT enough

• $D = [b_1, b_2, \ldots, b_n]$ in $\{0,1\}^n$

• Query $q$ returns sum of a subset in $D$

• Add bounded noise ($\leq E$) before releasing answer

• Can reconstruct $D$ up to $4E$ positions!

• Run query on all $2^n$ subsets in $D$

• Return any database $D'$ such that $\sup_S |D'(s) - q(S)| \leq E$
Nothing Personal
But how?

• Say, medical study about smoking causes cancer
• Should a smoker participate?
• If yes, may lead to higher insurance premium
• But may also benefit from learning health risks
• Has the smoker’s privacy been compromised?

Participate or not, the impact on the smoker would likely be the same
Have you cheated in any exam?
Randomized Response

- Want to estimate percentage of cheaters
  - so that we know the severity of this problem
- If ask bluntly, almost certainly will under-estimate
- Toss a coin: head, answer honestly; tail, answer randomly
  - cheater: w.p. 3/4 say yes
  - non-cheater: w.p. 1/4 say yes
  - $\frac{3}{4} \times p + \frac{1}{4} \times (1-p) = \text{percentage of yes}$
- Plausible deniability for each individual
A randomized algorithm $\mathcal{M}$ is $(\varepsilon, \delta)$-DP if for all $S \subseteq \text{Range}(\mathcal{M})$ and for all $\|D_1 - D_2\|_1 \leq 1$:
\[
\Pr[\mathcal{M}(D_1) \in S] \leq \exp(\varepsilon) \cdot \Pr[\mathcal{M}(D_2) \in S] + \delta
\]

- The smaller $(\varepsilon, \delta)$ are, the stricter the definition

- $\delta = 0$ is also used

\[
\left| \log \frac{\Pr[\mathcal{M}(D_1) \in S]}{\Pr[\mathcal{M}(D_2) \in S]} \right| \leq \varepsilon
\]
Exercise

A randomized algorithm $\mathcal{M}$ is $(\epsilon, \delta)$-DP if for all $S \subseteq \text{Range}(\mathcal{M})$ and for all $\|D_1 - D_2\|_1 \leq 1$:

$$\Pr[\mathcal{M}(D_1) \in S] \leq \exp(\epsilon) \cdot \Pr[\mathcal{M}(D_2) \in S] + \delta$$

• What if $\|D_1 - D_2\|_1 = k$?
DP never gets worse by post-processing

Let $\mathcal{M} : \mathcal{D} \rightarrow \mathcal{E}$ be $(\epsilon, \delta)$-DP and $\mathcal{N} : \mathcal{E} \rightarrow \mathcal{F}$ be any randomized mapping (not related to $\mathcal{M}$). Then $\mathcal{N} \circ \mathcal{M}$ is also $(\epsilon, \delta)$-DP.

• Conditioning on $\mathcal{N}$:

$$\Pr[\mathcal{N}(\mathcal{M}(D)) \in S] = \Pr[\mathcal{M}(D) \in \mathcal{N}^{-1}(S)]$$
RR is $(\ln 3, 0)$-DP

$$\log \left| \frac{\text{Pr}[\mathcal{M}(D_1) \in S]}{\text{Pr}[\mathcal{M}(D_2) \in S]} \right| \leq \epsilon$$
Laplace distribution

\[ p(x) = \frac{1}{2\lambda} \exp \left( -\frac{|x - \mu|}{\lambda} \right) \]
Given any function $f : \mathcal{D} \rightarrow \mathbb{R}^d$, the Laplacian mechanism returns:

$$\mathcal{M}_L(D, f, \epsilon) = f(D) + (Z_1, \ldots, Z_d),$$

where $Z_j$ are iid r.v. drawn from Laplace with

$$\lambda = \frac{\|
abla f\|_1}{\epsilon}.$$

**Laplacian Mechanism achieves ($\epsilon, 0$)-DP**

$$\log \frac{\Pr[\mathcal{M}_L(D_1) \in S]}{\Pr[\mathcal{M}_L(D_2) \in S]} \leq \sup_z \log \frac{p(f(D_1) - z)}{p(f(D_2) - z)}$$
Examples

• Counting queries

• Histogram queries
  • density estimation
Calculus of DP

Let $M_i : D_i \rightarrow E_i$ be $(\epsilon_i, \delta_i)$-DP. Then the product map

$M : \prod_i D_i \rightarrow \prod_i E_i$ is $(\epsilon, \delta)$-DP, where

$\epsilon = \sum_i \epsilon_i$, $\delta = \sum_i \delta_i$
Influence Function

Let $T : \mathcal{D} \to \mathbb{R}$ be a statistical functional. Its influence function at distribution $F \in \mathcal{D}$ and point $x \in \mathbb{R}^d$ is:

$$\text{IF}(T, F, x) = \lim_{t \to 0} \frac{T((1 - t)F + t\delta_x) - T(F)}{t}$$

$$\sup_{x \in \mathbb{R}^d} |\text{IF}(T, F, x)|$$ is a measure of robustness and privacy
Let $T : \mathcal{D} \rightarrow \mathbb{R}$ return the mean of the input distribution.

$$
\text{IF}(T, F, x) = \lim_{t \to 0} \frac{(1 - t)\mu_F + tx - \mu_F}{t}
$$

$$
\sup_{x \in \mathbb{R}^d} |\text{IF}(T, F, x)| \equiv \infty
$$