L21: Privacy

Jeff M. Phillips

April 6, 2020
Ethics = Empathy

What if you were the date point?

A = \text{what if this was you?}
In early 2000s, lot new tech companies eagerness, interact scientists.

Place data set online, among it, state goal, have competition to solve model, predictions.
Example: Heath Records

Story Time:

In 2000, Massachusetts released all State employee's medical records in an effort for researchers to be able to study them. They wiped all ids, but kept zip codes, birthday, gender. Was declared anonymized by the government.

In Massachusetts, it was possible to buy voter data for $20. It has names, zip codes, and gender of all voters.

A grad student, Latanya Sweeney combined the two to identify the governor of Massachusetts. Story is, she mailed him his own health records!

Dr. Sweeney now teaches at Harvard.
Example: Heath Records

**Story Time:**

- In 2000, Massachusetts released all State employee’s medical records in an effort for researchers to be able to study them.
Example: Heath Records

**Story Time:**
- In 2000, Massachusetts released all State employee’s medical records in an effort for researchers to be able to study them.
- They wiped all ids, but kept zip codes, birthday, gender. Was declared anonymized by the government.
Story Time:

- In 2000, Massachusetts released all State employee’s medical records in an effort for researchers to be able to study them.
- They wiped all ids, but kept zip codes, birthday, gender. Was declared anonymized by the government.
- In Massachusetts, it was possible to buy voter data for $20. It has names, zip codes, and gender of all voters.
Story Time:

- In 2000, Massachusetts released all State employee’s medical records in an effort for researchers to be able to study them.
- They wiped all ids, but kept zip codes, birthday, gender. Was declared anonymized by the government.
- In Massachusetts, it was possible to buy voter data for $20. It has names, zip codes, and gender of all voters.
- A grad student, Latanya Sweeney combined the two to identify the governor of Massachusetts. Story is, she mailed him his own health records!
Example: Heath Records

**Story Time:**
- In 2000, Massachusetts released all State employee’s medical records in an effort for researchers to be able to study them.
- They wiped all ids, but kept zip codes, birthday, gender. Was declared anonymized by the government.
- In Massachusetts, it was possible to buy voter data for $20. It has names, zip codes, and gender of all voters.
- A grad student, Latanya Sweeney combined the two to identify the governor of Massachusetts. Story is, she mailed him his own health records!
- *Dr.* Sweeney now teaches at Harvard.
How to release data anonymously while preserving individual info?

$k$-anonymity: data set has public traits

- age, zip code, gender (categorical)

private traits: has cancer, has Cove

enforce at least each person has at least $k-1$ other people with same publicly released traits.
l-diversity; k-anonymity; and each group had l-diverse traits. E.g., some have cancer, some don't.

Issue: either have cancer or have diabetes.

t-closeness; l-diversity and the distribution of traits is t-close to distribution of all people in data.
Height of Sylvester Stallone

- Information: Sly Stallone is height of the average NJ man.

- Independent survey: Average height of men in NJ is 5'8"
Example: Netflix Prize

**Story Time:**

In 2006, Netflix (e.g., DVDs) released awesome data sets $D_1 = \{ \text{user-id, movie, date of grade, grade} \}$ and another set $D_2 = \{ \text{user-id, movie, date of grade} \}$. Wants researchers to predict grade on $D_2$. (Had another similar private data $D_3$ to evaluate grades: cross validation.) If certain improvement over Netflix’s algorithm, get $1$ million! Led to lots of cool research! Raters of movies also rated on IMDB (w/ user id, time stamp) Researchers showed that by linking who rated similar sets of movies, with similar scores and times, they could identify many people. (Maybe watched embarrassing films on Netflix, not listed on IMDB.) Class action lawsuit filed (later dropped) against Netflix. Netflix Prize had proposed sequel, dropped in 2010 for more privacy concerns.
Example: Netflix Prize

Story Time:

- In 2006, Netflix (e.g., DVDs) released awesome data sets
  \( D_1 = \{ \langle \text{user-id}, \text{movie}, \text{date of grade}, \text{grade} \rangle \} \).
  And another set \( D_2 = \{ \langle \text{user-id}, \text{movie}, \text{date of grade} \rangle \} \).
  Wants researchers to predict grade on \( D_2 \).
  (Had another similar private data \( D_3 \) to evaluate grades: cross validation.)
Example: Netflix Prize

**Story Time:**

- In 2006, Netflix (e.g., DVDs) released awesome data sets $D_1 = \{(\text{user-id}, \text{movie}, \text{date of grade}, \text{grade})\}$. And another set $D_2 = \{(\text{user-id}, \text{movie}, \text{date of grade})\}$. Wants researchers to predict grade on $D_2$. (Had another similar private data $D_3$ to evaluate grades: cross validation.)
- If certain improvement over Netflix’s algorithm, get $1\text{ million}!$
Example: Netflix Prize

Story Time:

- In 2006, Netflix (e.g., DVDs) released awesome data sets $D_1 = \{\langle \text{user-id, movie, date of grade, grade} \rangle \}$. And another set $D_2 = \{\langle \text{user-id, movie, date of grade} \rangle \}$. Wants researchers to predict grade on $D_2$.
  (Had another similar private data $D_3$ to evaluate grades: cross validation.)
- If certain improvement over Netflix’s algorithm, get $1$ million!
- Led to lots of cool research!
Example: Netflix Prize

**Story Time:**

- In 2006, Netflix (e.g., DVDs) released awesome data sets $D_1 = \{\langle \text{user-id, movie, date of grade, grade} \rangle \}$. And another set $D_2 = \{\langle \text{user-id, movie, date of grade} \rangle \}$. Wants researchers to predict grade on $D_2$. (Had another similar private data $D_3$ to evaluate grades: cross validation.)
- If certain improvement over Netflix’s algorithm, get $1$ million!
- Led to lots of cool research!
- Raters of movies also rated on IMDB (w/ user id, time stamp)
Example: Netflix Prize

**Story Time:**

- In 2006, Netflix (e.g., DVDs) released awesome data sets $D_1 = \{\langle \text{user-id, movie, date of grade, grade} \rangle \}$. And another set $D_2 = \{\langle \text{user-id, movie, date of grade} \rangle \}$. Wants researchers to predict grade on $D_2$. (Had another similar private data $D_3$ to evaluate grades: cross validation.)
- If certain improvement over Netflix’s algorithm, get $1$ million!
- Led to lots of cool research!
- Raters of movies also rated on IMDB (w/ user id, time stamp)
- Researchers showed that by linking who rated similar sets of movies, with similar scores and times, they could identify many people.
Example: Netflix Prize

Story Time:

- In 2006, Netflix (e.g., DVDs) released awesome data sets $D_1 = \{\langle \text{user-id}, \text{movie}, \text{date of grade}, \text{grade} \rangle \}$. And another set $D_2 = \{\langle \text{user-id}, \text{movie}, \text{date of grade} \rangle \}$. Wants researchers to predict grade on $D_2$. (Had another similar private data $D_3$ to evaluate grades: cross validation.)
- If certain improvement over Netflix’s algorithm, get $1$ million!
- Led to lots of cool research!
- Raters of movies also rated on IMDB (w/ user id, time stamp)
- Researchers showed that by linking who rated similar sets of movies, with similar scores and times, they could identify many people.
- (maybe watched embarrassing films on Netflix, not listed on IMDB)
Example: Netflix Prize

Story Time:

- In 2006, Netflix (e.g., DVDs) released awesome data sets $D_1 = \{\text{user-id, movie, date of grade, grade}\}$.
- And another set $D_2 = \{\text{user-id, movie, date of grade}\}$.
- Wants researchers to predict grade on $D_2$.
- (Had another similar private data $D_3$ to evaluate grades: cross validation.)
- If certain improvement over Netflix’s algorithm, get $1$ million!
- Led to lots of cool research!
- Raters of movies also rated on IMDB (w/ user id, time stamp)
- Researchers showed that by linking who rated similar sets of movies, with similar scores and times, they could identify many people.
- (maybe watched embarrassing films on Netflix, not listed on IMDB)
- Class action lawsuit filed (lated dropped) against Netflix.
Example: Netflix Prize

**Story Time:**

- In 2006, Netflix (e.g., DVDs) released awesome data sets $D_1 = \{\langle \text{user-id, movie, date of grade, grade} \rangle \}$. And another set $D_2 = \{\langle \text{user-id, movie, date of grade} \rangle \}$.
- Wants researchers to predict grade on $D_2$.
- (Had another similar private data $D_3$ to evaluate grades: cross validation.)
- If certain improvement over Netflix’s algorithm, get $1$ million!
- Led to lots of cool research!
- Raters of movies also rated on IMDB (w/ user id, time stamp)
- Researchers showed that by linking who rated similar sets of movies, with similar scores and times, they could identify many people.
- (maybe watched embarrassing films on Netflix, not listed on IMDB)
- Class action lawsuit filed (lately dropped) against Netflix.
- Netflix Prize had proposed sequel, dropped in 2010 for more privacy concerns.
Differential Privacy

Two similar data sets $D_1$ & $D_2$

$\Delta$ global analysis on $D_1$ similar to $D_2$

$\Delta$ for no particular data point in $D_1$ can I know its value.

Global analysis

$\forall g \in \mathbb{Q}$

$\Pr[\mathbb{E}[g(D_1)] \in \mathbb{R}] \leq \exp(\epsilon) \approx 1.4$
Two Versions

Interactive Version

I control $D_1$, $D_2$

I limit queries

I return answer w/ noise

$D_1$, $D_2$

Change $D_2$ as I go.

Non-Interactive

I perturb $D_1 \rightarrow D_2$

I release $D_2$.

$D_2 = \text{Dirt Lap Noise}$
Height of Sly Stallone

\[ D_2 = 5'9'' = 69'' = D_1 + \text{lap} (\alpha) \]

\[ \text{Example: } D_1 = 68'' \]

\[ P_c [D_1 \geq 70] = e^{-2\alpha} \]

\[ P_c [D_2 \geq 70] = e^{-\alpha} \]

\[ \frac{P_c [D_2 \geq 70]}{P_c [D_1 \geq 70]} = e^{\alpha} = 1 + \alpha \]