Towards **User-oriented** privacy for recommender system data: A **personalization**-based approach to gender **obfuscation** for user profiles

Manel Slokom

E-mail: m.slokom@tudelft.nl
Twitter: @ManelSlokom

Delft University of Technology, The Netherlands
The Sim4IR Workshop at SIGIR 2021

July 15, 2021
<table>
<thead>
<tr>
<th>Users</th>
<th>$i_1$</th>
<th>$i_2$</th>
<th>$i_3$</th>
<th>$i_4$</th>
<th>$i_5$</th>
<th>$i_6$</th>
<th>$i_7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_1$</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$u_2$</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$u_3$</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>$u_4$</td>
<td>5</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>$u_5$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>
Framework

Input  Obfuscation  Output
Framework

Input

Obfuscation

Output

$Rec^{Original}$

$Rec^{Obfuscated}$

Recommendation Performance
In the table: we used ML1M data set. PerBlur is created with addition from the personalized lists of indicative items.
Framework

- **Input**
- **Obfuscation**
- **Output**

- $Rec^{Original}$
- $Rec^{Obfuscated}$

**Recommendation Performance**

**Inference attack**

*Extent to which Gender Inference is Blocked*
In the table: we used ML1M data set. **PerBlur** is created with *addition* from the *personalized* lists of indicative items. Logistic regression classifier.
Take home message

• A simple, yet effective **personalized**-based approach to gender **obfuscation** for user profiles

• A recommender system trained on the obfuscated data is able to reach performance **comparable** to what is attained when trained on the original data

• A classifier can **no longer** reliably predict the gender of users

• The ability to recommend **diverse** items.
PerBlur - Personalized Blurring

- PerBlur creates the *personalized lists* of indicative items by intersecting:
  - Two lists of indicative items: $L_m$ and $L_f$
  - A personalized list of items ranked in order of the probability that the user will have rated them.

- **Standard PerBlur**
  - Obfuscation by *adding* extra items from the personalized lists of indicative items
  - Level of obfuscation.

- **PerBlur with removal**
  - Similar to *Standard PerBlur* but we also *remove* certain items.
Gender inference

1% Extra Ratings

2% Extra Ratings

5% Extra Ratings
Gender inference

- Obfuscation inhibits the inference of the gender
- PerBlur requires less obfuscation
- Transferability

<table>
<thead>
<tr>
<th>Personalization</th>
<th>Logistic regression</th>
<th>SVM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td><strong>BlurMe</strong></td>
<td>None</td>
<td>0.87</td>
</tr>
<tr>
<td><strong>PerBlur</strong></td>
<td>Personalized</td>
<td>0.87</td>
</tr>
</tbody>
</table>

In the table, we report the AUC scores on ML1M data set. **BlurMe** is created with addition from $L_m$ or $L_f$. **PerBlur** is created with addition from the personalized lists of indicative items.
The recommendation performance comes close to what is achieved on original data. PerBlur, thanks to its *personalization*, approaches the original performance more closely and more consistently than BlurMe.

<table>
<thead>
<tr>
<th></th>
<th>nDCG</th>
<th>HR@10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original</td>
<td>0.1634</td>
<td>0.1712</td>
</tr>
<tr>
<td>BlurMe</td>
<td>0.1536</td>
<td>0.1633</td>
</tr>
<tr>
<td>PerBlur</td>
<td>0.1637</td>
<td>0.1704</td>
</tr>
</tbody>
</table>

In the table: we used BPRMF algorithm on ML1M data set. **BlurMe** is created with *addition* from $L_m$ or $L_f$. **PerBlur** is created with *addition* from the *personalized* lists of indicative items.
Achieving diverse results

- The proportion of correctly recommended items that are stereotypical for gender
- Three different cutoff levels (10, 20, 50)

<table>
<thead>
<tr>
<th>Obfuscation Strategy</th>
<th>Gender-sterotypical items</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>top10F</td>
</tr>
<tr>
<td>Original</td>
<td>None</td>
</tr>
<tr>
<td>PerBlur</td>
<td>Personalized</td>
</tr>
</tbody>
</table>

- PerBlur is effective in lowering the proportion of TopN gender-sterotypical items

In the table: we used ML1M data set. PerBlur is created with addition from the personalized lists of indicative items and removal from $L_m$ or $L_f$. 
Outlook and future work

1. Data obfuscation for recommender systems
2. Step toward **data sharing** without privacy concerns
3. From privacy to **fairness** and **diversity**
4. From **partially** to **fully** synthetic data
Thank You
References

Manel Slokom, Martha Larson and Alan Hanjalic (2021)
Under review.

Manel Slokom, Martha Larson, and Alan Hanjalic (2019)
In: Late-Breaking Results RecSys’19. pp. 21-25.

Christopher Strucks, Manel Slokom, and Martha Larson (2019)
BlurM(or)e: Revisiting gender obfuscation in the user-item matrix.
Recommendation in Multistakeholder Environments in conjunction with the 13th ACM Conference on Recommender Systems (RecSys’19).

Manel Slokom (2018)
Comparing recommender systems using synthetic data