Differentially Private and Fair Algorithmic Hiring

Anonymous Author(s)

ABSTRACT

This paper investigates the trade-offs between effectiveness, fairness, and privacy in job recommender systems that suggest job seekers for specific job postings. We assume that the system cannot be trusted with sensitive attributes of job seekers (e.g., nationality, gender), yet it must still ensure fair representation of all sensitive groups in the recommendation list. This creates a fundamental tension between fairness and privacy. To address this, we propose a novel framework that enhances fairness even when sensitive attributes are perturbed using a local differential privacy mechanism. Extensive experiments on real-world job platform data demonstrate that our framework can maintain fairness, even under strong privacy constraints.

CCS CONCEPTS

• **Information systems → Recommender systems**.

KEYWORDS

Group fairness, Job Recommendations, Differential Privacy

ACM Reference Format:

Anonymous Author(s). 2025. Differentially Private and Fair Algorithmic Hiring. In *19th ACM Conference on Recommender Systems Prague, Czech Republic, September 22–26, 2025*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Job recommender systems have become vital in the recruitment process, facilitating the efficient matching of job seekers with job postings that align with their qualifications and preferences. In this context, the system's task is to recommend a set of suitable job seekers (acting as *items*, in recommender system terminology) for a given job posting (acting as the *user*). This task raises fairness concerns related to the treatment of job seekers [14]. Specifically, the system should not discriminate against job seekers based on *protected* attributes, such as membership in demographic minorities or residence in underrepresented regions. This item-side[1] notion of recommendation fairness [6] has been extensively studied, particularly in the context of job recommenders [7]. A common approach to ensuring fairness for job seekers is post-processing, where the recommendation list is reranked based on protected attributes.

For a fairness mitigation algorithm to function effectively, it must have access to the protected attributes of job seekers. However, this requirement is often unrealistic, as these attributes are typically also *sensitive*. Job seekers may be unwilling to disclose such information, or the system may be legally prohibited from collecting it under regulations such as the GDPR [17]. This creates a catch-22: to uphold privacy, the system refrains from collecting sensitive and protected attributes—yet without this information, it becomes impossible to guarantee fairness for job seekers. We call this the *private-but-not-fair* scenario: privacy is upheld—the recommender collects no sensitive information—but fairness is sacrificed.

In this paper, we investigate a more desirable alternative that upholds both the privacy and fairness of job seekers; we call this the *private-and-fair* scenario. We propose the use of a Local Differential Privacy (LDP) mechanism to ensure that the recommender, which cannot be trusted, never sees the actual sensitive attributes of the job seekers. Specifically, LDP perturbs the protected attributes of job seekers *before* they are sent to the recommender, ensuring thus privacy. Next, the recommender applies a fairness mitigation algorithm based on the perturbed, and hence noisy, protected attributes. Because LDP adds noise in a randomized yet structured manner, the fairness mitigation algorithm is still able to assure fairness.

We present the LDP-FAIR framework, which implements the *private-and-fair* scenario. LDP-FAIR operates in three phases. In the *Privacy Phase*, an LDP mechanism perturbs each job seeker's sensitive information, before sharing it with the recommender system. In the *Recommendation Phase*, given a job posting, the system recommends a ranked list of job seekers. In the *Fairness Phase*, this list is reranked to ensure fairness. The reranking algorithm accesses only the perturbed protected attributes. Note that the first phase is executed on each job seeker's device, while the last two phases are carried out by the untrusted job recommender system.

We materialize LDP-FAIR using different options for each phase. For the privacy phase, we investigate two LDP mechanisms: randomized response [19] and unary encoding [18]. For the recommendation phase, we consider two recommenders: BPR [13] and NeuMF [8]. For the fairness phase, we employ three reranking algorithms: DetGreedy, DetCons, and DetRelax [7].

To assess the effectiveness of fairness mitigation under privacy constraints, we consider a hypothetical *fair-but-not-private* scenario. In this scenario, privacy is sacrificed, and since the system has access to the raw protected attributes, it is able to maximize fairness mitigation, serving thus as the ideal scenario for fairness.

We conduct experiments on two job recommendation datasets, yielding the following key findings. Compared to the *fair-but-not-private* scenario, which maximizes fairness, LDP-FAIR achieves comparable fairness even under strong privacy guarantees. Compared to the *private-but-not-fair* scenario, LDP-FAIR provides controllable privacy loss, maintains comparable recommendation effectiveness, and significantly improves fairness in job recommendations.

[1] Item-side, or provider, fairness [5] pertains to the individuals associated with the recommended items—such as their producers, owners, or, as in our case, the individuals represented by the items themselves. In contrast, user-side, or consumer, fairness [6] focuses on the individuals receiving the recommendations—that is, the end-users or consumers.

RecSys '25, September 22–26, 2025, Prague, Czech Republic

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

2 RELATED WORK

Fairness in Recommender Systems. Geyik et al. [7] proposed a family of fairness-aware algorithms (DetGreedy, DetRelax, and DetCons), which rerank an existing list of job seekers to ensure an equal representation of each state/value (e.g., male or female) of an attribute (e.g. gender) inside the job recommendation list. In the same direction, Li et al. [11] addressed fairness concerns in recommender systems under a premium user scenario. The authors proposed a novel metric to quantify fairness in the context where premium users are present and introduced a flexible, contextual fairness-aware recommendation framework. This framework incorporates a desired distribution to align with the score distributions of user or item groups. Moreover, Rus et al. [14] provided unbiased job recommendations by removing gender bias from word embeddings of job postings and user resumes. The authors have showed experimentally that their job recommendations, which are based on these word embeddings, can mitigate the salary difference that exists between the jobs of women and men that have equal job qualifications. Finally Abdollahpouri et al. [2] studied the relationship between popularity bias, calibration, and fairness in recommendation systems. They found that recommendation algorithms tend to exhibit a popularity bias, which can lead to miscalibration. This miscalibration can disproportionately affect certain user groups, resulting in unfair treatment.

Our work directly relates to the fairness concerns in job recommendation as expressed in [7]. Therefore, in our framework, we include their fairness-aware algorithms.

Privacy in Recommender Systems. Jiang et al. [10] extended the NeuMF [8] algorithm and build a federated learning recommender system, denoted as FedNCF. The paper of Yang et al. [22] proposed a differential privacy (DP) framework for collaborative filtering-based algorithms, denoted as DP-Fair, which combines differential privacy mechanisms with fairness constraints to protect user privacy while ensuring fair recommendations. Their experiments demonstrate that DP-Fair exhibits superior performance in terms of both overall accuracy and user group fairness compared to differential private stochastic gradient descent (DP-SGD). The work of Slokom et al. [15] proposes a privacy-preserving solution for the data used to train a recommender system. Their solution, denoted as Personalized Blurring (PerBlur), is a simple and effective approach, which adds and removes items from users' profiles in order to generate an obfuscated user–item rating matrix. Finally, the paper by Müllner et al. [12] investigates the ways in which DP impacts personalized recommendations. Their experiments with different datasets and recommendation algorithms show that adding DP to the training data (user-item interactions) substantially reduces recommendation accuracy while increasing popularity bias.

We emphasize that all these methods assume that the recommender system can be trusted, and thus it is given full access to sensitive data. Their goal is to train a recommendation model that does not leak sensitive data. Thus they employ DP techniques *during* training. In contrast, our privacy requirements are stronger, as we want the recommender to not have access to sensitive data. Thus we apply LDP techniques to protect privacy *before* training.

3 LOCAL DIFFERENTIAL PRIVACY

This section describes the LDP mechanisms used in LDP-FAIR, both of which are applicable to categorical sensitive attributes with domains comprising multiple values—for example, the nationality, race, or gender of a job seeker. Their goal is to protect the actual sensitive attribute value by either (i) replacing it with another in the domain (the GRR approach), or by (ii) hiding it among a set of values in the domain (the UE approach). Both use two parameters p, q but with different semantics. And both offer a differential privacy guarantee of ϵ expressed as a function of p, q.

Formally, consider an LDP mechanism f that takes a value x from the sensitive attribute domain X and transforms it into an output $y \in \text{Range}(f)$, the set of all possible outputs of f. We say that f satisfies ϵ-local differential privacy, for $\epsilon > 0$, if for all $x_1, x_2 \in X$ and for all $y \in \text{Range}(f)$, it holds that:

$$Pr[f(x_1) = y] \leq e^{\epsilon} Pr[f(x_2) = y].$$

Intuitively, this means that the output distribution of f does not differ too much across different inputs: as ϵ approaches 0, the distributions become indistinguishable, making it increasingly difficult to infer whether a particular output y was generated from x_1 or x_2.

Generalized Randomized Response. Generalized Randomized Response (GRR) [19] is a generalized version of the classic Randomized Response technique [20]. GRR enables individuals to respond to queries without directly revealing their sensitive information. The key requirement of GRR is that, for any possible response, the probability of reporting that response should not differ by more than a multiplicative factor of e^{ϵ}, thereby ensuring differential privacy. The probability of changing a value of a sensitive attribute to another value of the same attribute is defined as follows: (i) Keep an attribute's value unchanged with probability p, and (ii) Change an attribute's value with probability q. The level of privacy protection is quantified by the privacy loss parameter ϵ, which is calculated using Equation 1:

$$\epsilon = \ln \max \left\{ \frac{p}{q}, \frac{q}{p} \right\}. \tag{1}$$

Unary Encoding. The Unary Encoding (UE) method [18] views a categorical domain as a unary-encoded binary vector, where each bit corresponds to a value in the domain. UE perturbs each bit independently with a fixed probability. This controlled bit-flipping mechanism introduces randomness, thereby safeguarding individual privacy while preserving the utility of the data. The probability of flipping a bit is defined as follows: (i) For a bit that is 1, it is kept as 1 with probability p and flipped to 0 with probability $1 - p$. (ii) For a bit that is 0, it is kept as 0 with probability $1 - q$ and flipped to 1 with probability q. The privacy guarantee ϵ is computed with Equation 2:

$$\epsilon = \ln \max \left\{ \frac{p(1-q)}{q(1-p)}, \frac{q(1-p)}{p(1-q)} \right\}. \tag{2}$$

4 THE LDP-FAIR FRAMEWORK

In this section, we introduce the LDP-FAIR framework, which is described in Algorithm 1. LDP-FAIR seeks to ensure fairness under privacy constraints.

Algorithm 1 1: The LDP-FAIR Framework

Input: `SensitiveData`: The set of sensitive attributes for all job seekers; `InteractionData`: Historical interaction data of job seekers with job postings; ϵ: Desired privacy loss.
Output: `RerankedRecommendationList`: The private and fair job seeker recommendation list for each job posting.

1 **Step 1 (Privacy).** Apply an LDP mechanism (e.g., GRR, UE) to each sensitive attribute on each job seeker individually. Select p and q so that the desired privacy loss of ϵ is guaranteed. The output is a perturbed version of the raw `SensitiveData`, which we refer to as `PrivateSensitiveData`, Send `PrivateSensitiveData` to the recommender.
2 **Step 2 (Recommendation).** The recommender system trains a model (e.g., NeuMF, BPR) on the job seekers `InteractionData`. Then, for each job posting, the recommender proposes a list of job seekers `RecommendationList`.
3 **Step 3 (Fairness).** The recommender system applies a reranking algorithm (e.g., DetGreedy, DetCons, DetRelax) on each `RecommendationList` that operates on the `PrivateSensitiveData`. Reranking produces a `RerankedRecommendationList` where the distribution of `PrivateSensitiveData` is fair. For example, it tries to ensure job seekers from all perturbed nationalities appear in `RerankedRecommendationList`; note that the reranking algorithm only sees the perturbed nationalities.
4 **return** `RerankedRecommendationList`

In Step 1, LDP-FAIR applies a local differential privacy mechanism to introduces noise into the job seekers sensitive attributes, which are required to ensure fairness.

In Step 2, given a job posting, the recommender generates an initial ranking of job seekers using a baseline recommendation algorithm (e.g., NeuMF [8], BPR[13]). We note that the job seekers sensitive attributes are not used in this step.

Finally, in Step 3, the system reranks the recommendation list to improve fairness for job seekers. A *group* refers to job seekers who share the same sensitive attribute values, such as nationality or gender. The goal is to ensure that all such groups are fairly represented in the final list of recommendations.

For the last step, a reranking algorithm from [7] is used. Among the available strategies, DetGreedy takes a greedy approach: it selects highly relevant job seekers while addressing imbalances by prioritizing job seekers from underrepresented groups. It does this by swapping in such job seekers to improve group representation, without strictly enforcing fairness constraints. In contrast, DetCons is more rigorous. It prioritizes job seekers whose groups are at the greatest risk of not meeting minimum representation requirements. Finally, DetRelax is a relaxed version of DetCons that allows small deviations from the fairness constraints, trading strict fairness for improved ranking quality.

In summary, our LDP-FAIR framework ensures fairness while protecting job seekers sensitive data.

5 EXPERIMENTAL EVALUATION

We have uploaded the full python code and the outputs of our LDF-FAIR algorithm in the following anonymized repository: https://anonymous.4open.science/r/ldp-fair-A028.

5.1 Data Sets

Our first dataset, originally used in RecSys Challenge 2016 [3, 4] and the data were provided by XING. Henceforth, we will refer to this as the XING16 dataset. XING16 dataset contains 8,826,678 interactions of 1,367,057 job seeker with 1,358,098 job postings. It also contains content features about job seeker (*region, industry_id*, etc.) and job postings (*region, industry_id,* etc.). CareerBuilder12 originally used in an open Kaggle competition [1], called Job Recommendation Challenge, provided by the online employment Web site CareerBuilder. CareerBuilder12 dataset contains 661,910 interactions of 120,147 job seeker with 197,590 job postings. It also contains content features about job seeker (*State, Topic,* etc.) and job postings (*State, Country,* etc.).

5.2 Evaluation Metrics

Given a job posting, the job recommender compiles a recommendation list containing job seekrs, which is then reranked for fairness. To evaluate the effectiveness of a recommendation list, we use classic metrics, such as normalized Discounted Cumulative Gain (nDCG) [9], Mean Reciprocal Rank (MRR) [21].

To evaluate the impact of reranking, we define the Utility metric $\mathcal{U}$ that measures how different the fairness-aware reranked list is compared to the original recommendation list, which is ranked based on the recommender's predicted relevance of a job seeker to the given job posting. Specifically, let $\hat{rel}_u(t)$ denote the *predicted relevance* of job seeker t to job posting u; in our context, job seekers are the items, and job postings are the users. Then, given a recommendation list R_u, we define its utility for job posting u as the nDCG computed on the predicted relevance:

$$\mathcal{U}(R_u) = \frac{1}{\mathcal{U}_u^*} \sum_{i=1}^{|R_u|} \frac{\hat{rel}_u(R_u[i])}{\log_2(i+1)}, \tag{3}$$

where $\mathcal{U}_u^*$ is the highest possible utility for job posting u. The utility of a set $\mathbb{R}$ of recommendation lists is simply the mean:

$$\mathcal{U}(\mathbb{R}) = \frac{1}{|\mathbb{R}|} \sum_{R_u \in \mathbb{R}} \mathcal{U}(R_u). \tag{4}$$

Please note that the initial recommendation list returned in step 2 of Algorithm 1 is considered as having always perfect utility $\mathcal{U}(R_u) = 1$. Thus this utility metric is primarily meaningful for indicating relative changes in accuracy before and after the application of reranking.

Finally, to evaluate job seeker fairness, we use Normalized Discounted KL-divergence (nDKL) [7, 16], which measures how closely the distribution of sensitive attributes in the recommendation list aligns with a desired fair distribution. For example, we might want each nationality to be equally represented in the recommendation list. nDKL quantifies how well this fairness criterion is met at each prefix of the list. The nDKL metric is non-negative with smaller values being more preferable. Note that we compute nDKL using the real sensitive job seeker data, as our goal is to quantify the impact of privacy on fairness, as the fairness-aware reranking only sees perturbed sensitive values.

5.3 Evaluation Results

In this subsection, we evaluate the performance of the fairness-aware algorithms DetGreedy, DetRelaxed, DetCons [7], together with a base NeuMF [8] algorithm, using real-world data from the XING16 and CareerBuilder12 platforms. In all experiments, the base recommender is NeuMF [8], but we have verified analogous results with the Bayesian Personalized Ranking (BPR) algorithm [13]. The

Table 1: Algorithms' comparison for different privacy levels on two different datasets.

		XING16							CareerBuilder12						
		NeuMF	DetGreedy		DetCons		DetRelax		NeuMF	DetGreedy		DetCons		DetRelax	
			UE	GRR	UE	GRR	UE	GRR		UE	GRR	UE	GRR	UE	GRR
No Privacy ($\epsilon = \infty$)															
Effectiveness	nDGG@30 (↑)	**0.30**	0.30		0.21		0.29		**0.13**	0.11		0.08		0.11	
	$\mathcal{U}$@30 (↑)	**1.00**	0.97		0.70		0.95		**1.00**	0.90		0.65		0.89	
	MRR@30 (↑)	0.21	0.22		**0.29**		**0.29**		**0.14**	**0.14**		0.14		0.14	
Fairness	nDKL@30 (region) (↓)	2.65	**2.59**		2.57		**2.56**		2.55	2.45		2.51		**2.42**	
Low Privacy ($\epsilon = 9.8$)															
Effectiveness	nDGG@30 (↑)	**0.30**	**0.30**	**0.30**	0.20	0.21	0.21	0.29	**0.13**	0.11	0.11	0.07	0.08	0.09	0.11
	$\mathcal{U}$@30 (↑)	**1.00**	0.98	0.97	0.67	0.70	0.68	0.95	**1.00**	0.93	0.90	0.53	0.65	0.68	0.89
	MRR@30 (↑)	0.21	0.21	0.22	0.04	**0.29**	0.04	**0.29**	**0.14**	**0.14**	**0.14**	0.02	**0.14**	0.02	**0.14**
Fairness	nDKL@30 (region) (↓)	2.65	2.64	2.59	2.78	2.57	2.74	**2.56**	2.55	2.51	2.45	2.67	2.51	2.56	**2.42**
Medium Privacy ($\epsilon = 3.5$)															
Effectiveness	nDGG@30 (↑)	**0.30**	0.30	0.30	0.18	0.22	0.18	0.29	**0.13**	0.12	0.12	0.06	0.08	0.08	0.11
	$\mathcal{U}$@30 (↑)	**1.00**	0.99	0.97	0.59	0.71	0.67	0.95	**1.00**	0.98	0.92	0.51	0.66	0.66	0.91
	MRR@30 (↑)	0.21	0.21	0.21	0.06	**0.27**	0.07	**0.27**	**0.14**	**0.14**	**0.14**	0.04	0.13	0.04	0.13
Fairness	nDKL@30 (region) (↓)	2.65	2.65	2.60	2.90	2.59	2.67	**2.57**	2.55	2.53	2.46	2.76	2.50	2.63	**2.42**
High Privacy ($\epsilon = 1.2$)															
Effectiveness	nDGG@30 (↑)	**0.30**	**0.30**	**0.30**	0.16	0.22	0.19	0.29	**0.13**	0.12	0.12	0.06	0.09	0.07	0.12
	$\mathcal{U}$@30 (↑)	**1.00**	0.99	0.98	0.54	0.73	0.61	0.96	**1.00**	0.99	0.98	0.50	0.72	0.58	0.95
	MRR@30 (↑)	**0.21**	**0.21**	**0.21**	0.06	0.18	0.08	0.19	**0.14**	**0.14**	**0.14**	0.03	0.10	0.05	0.11
Fairness	nDKL@30 (region) (↓)	2.65	2.66	2.62	2.96	2.62	2.87	**2.59**	2.55	2.55	2.49	2.85	2.48	2.73	**2.43**

comparison focuses on descrided evaluation metrics, under different privacy levels applied via LDP methods (GRR [19] and UE [18]). We conduct all experiments using double cross-validation. In each outer fold, the data is split into 80% for training and 20% for testing. The 80% training portion is then further partitioned into 70% for actual training and 10% for validation, which is used to perform grid search for hyperparameter optimization. The default size of the recommendation list N is set to 30. The presented measurements, based on two-tailed t-test, are statistically significant at the 0.05 level. For XING16 dataset, the number of latent factors, the learning rate, and the layers for NeuMF is set to 10, 0.001, and [64, 32, 16, 8], respectively. For CareerBuilder12, the number of latent factors for NeuMF is set to 6, whereas the rest two parameters are similar to those of XING16 dataset. Table 1 show the results of the experiments on XING16 and CareerBuilder12 datasets, accordingly.

As can be seen in Table 1, the base recommender is NeuMF. We have to highlight that it is not a fairness-aware algorithm. That is, NeuMF does not use the protected attribute of region/State to produce job candidates recommendations. In terms of effectiveness metrics, as expected NeuMF has the highest performance in both datasets/Tables, but, as expected, it has very low performance in terms of fairness. Next, we test the performance of the fairness-aware algorithms, DetGreedy, DetCons, and DetRelax, in terms of effectiveness and fairness metrics, as we increase the level of privacy protection ranging from "No Privacy" ($\epsilon = \infty$) to "High Privacy" ($\epsilon = 1.2$), for the two LDP methods, UE and GRR. i.e., Unary Encoding (UE) and Generalized Randomized Response (GRR). In terms of effectiveness metrics, as we increase the privacy level in Table 1, we can observe that the effectiveness metrics tend to worsen for all fairness-aware algorithms when applying the UE method and tend to improve when applying the GRR method, except DetGreedy, which demonstrates robustness in maintaining or even increasing effectiveness/accuracy with high privacy levels, regardless of the LDP method used. In terms of the fairness metrics, as we increase the privacy level in Table 1, we can observe that the fairness metrics tend to worsen for all algorithms. Although the fairness metric tends to worsen with higher privacy (lower ϵ values), the DetRelax combined with GRR demonstrates better robustness than other algorithms in maintaining fairness. That is, in Table1, the nDKL@30 score of DetRelax rises from 2.56 in the "No Privacy" condition to 2.59 in "High Privacy". Similarly, in the Career Builder dataset, which can be seen in Table 1, DetRelax in the GRR setting has an increase from 2.42 to 2.43.

In summary, our experiments show that by increasing the privacy level, we worsen the fairness of the recommendations, while the results in accuracy show a different trend in each LDP method used. The nDKL metric, which estimates the fairness of an algorithm, consistently shows better values for DetRelax against all other algorithms. Henceforth, for the rest experimetns DetRelax along with GRR is our preferred combination. The main reason is that the GRR privacy method leads to more realistic approximations of the original distribution of the protected attribute (in our case the region of residence of the job candidates) than UE does.

6 CONCLUSION

This paper presents a detailed experimental comparison of fair reranking algorithms—DetGreedy, DetRelax, and DetCons—in combination with a job recommendation model such as NeuMF [8] and incorporating two Local Differential Privacy (LDP) techniques: Unary Encoding (UE)[19] and Generalized Randomized Response (GRR)[19]. The study assesses the trade-offs between fairness, effectiveness, and privacy, highlighting the relative strengths and limitations of each approach.

Using two real-world datasets—CareerBuilder12 and XING16—we show that the combination of the GRR method with the DetRelax reranking algorithm [7] consistently outperforms NeuMF and other fair reranking methods, especially under high privacy constraints.

REFERENCES

[1] 2012. Kaggle Job Recommendation Challenge. https://kaggle.com/competitions/job-recommendation Accessed: 2025-01-03.

[2] Himan Abdollahpouri, Mehdi Mansoury, Robin Burke, and Bamshad Mobasher. 2020. The Connection Between Popularity Bias, Calibration, and Fairness in Recommendation. In *Fourteenth ACM Conference on Recommender Systems (RecSys '20)* (Virtual Event, Brazil). ACM.

[3] Fabian Abel, András Benczúr, Daniel Kohlsdorf, Martha Larson, and Róbert Pálovics. 2016. RecSys challenge 2016: Job recommendations. In *Proceedings of the 10th ACM conference on recommender systems*. 425–426.

[4] Fabian Abel, Yashar Deldjoo, Mehdi Elahi, and Daniel Kohlsdorf. 2017. RecSys Challenge 2017: Offline and Online Evaluation. In *Proceedings of the Eleventh ACM Conference on Recommender Systems* (Como, Italy) *(RecSys '17)*. Association for Computing Machinery, New York, NY, USA, 372–373. https://doi.org/10.1145/3109859.3109954

[5] Robin Burke. 2017. Multisided Fairness for Recommendation. *CoRR* abs/1707.00093 (2017). arXiv:1707.00093 http://arxiv.org/abs/1707.00093

[6] Yashar Deldjoo, Dietmar Jannach, Alejandro Bellogin, Alessandro Difonzo, and Dario Zanzonelli. 2023. Fairness in recommender systems: research landscape and future directions. *User Modeling and User-Adapted Interaction* 34, 1 (April 2023), 59–108. http://dx.doi.org/10.1007/s11257-023-09364-z

[7] Sahin Cem Geyik, Stuart Ambler, and Krishnaram Kenthapadi. 2019. Fairness-Aware Ranking in Search & Recommendation Systems with Application to LinkedIn Talent Search. In *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (Anchorage, AK, USA) *(KDD '19)*. Association for Computing Machinery, New York, NY, USA, 2221–2231. https://doi.org/10.1145/3292500.3330691

[8] Xiangnan He, Lizi Liao, Hanwang Zhang, Liqiang Nie, Xia Hu, and Tat-Seng Chua. 2017. Neural Collaborative Filtering. In *Proceedings of the 26th International Conference on World Wide Web* (Perth, Australia) *(WWW '17)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 173–182. https://doi.org/10.1145/3038912.3052569

[9] Kalervo Järvelin and Jaana Kekäläinen. 2002. Cumulated gain-based evaluation of IR techniques. *ACM Trans. Inf. Syst.* 20, 4 (Oct. 2002), 422–446. https://doi.org/10.1145/582415.582418

[10] Xueyong Jiang, Baisong Liu, Jiangcheng Qin, Yunchong Zhang, and Jiangbo Qian. 2022. FedNCF: Federated Neural Collaborative Filtering for Privacy-preserving Recommender System. *2022 International Joint Conference on Neural Networks (IJCNN)* (2022), 1–8. https://api.semanticscholar.org/CorpusID:252625848

[11] Yangkun Li, Mohamed-Laid Hedia, Weizhi Ma, Hongyu Lu, Min Zhang, Yiqun Liu, and Shaoping Ma. 2022. Contextualized Fairness for Recommender Systems in Premium Scenarios. *Big Data Res.* 27, C (Feb. 2022), 7 pages. https://doi.org/10.1016/j.bdr.2021.100300

[12] Peter Müllner, Elisabeth Lex, Markus Schedl, and Dominik Kowald. 2024. The Impact of Differential Privacy on Recommendation Accuracy and Popularity Bias. arXiv:2401.03883 [cs.IR] https://arxiv.org/abs/2401.03883

[13] Steffen Rendle, Christoph Freudenthaler, Zeno Gantner, and Lars Schmidt-Thieme. 2009. BPR: Bayesian Personalized Ranking from Implicit Feedback. In *UAI 2009, Proceedings of the Twenty-Fifth Conference on Uncertainty in Artificial Intelligence, Montreal, QC, Canada, June 18-21, 2009*, Jeff A. Bilmes and Andrew Y. Ng (Eds.). AUAI Press, 452–461. https://www.auai.org/uai2009/papers/UAI2009_0139_48141db02b9f0b02bc7158819ebfa2c7.pdf

[14] Clara Rus, Jeffrey Luppes, Harrie Oosterhuis, and Gido H. Schoenmacker. 2022. Closing the Gender Wage Gap: Adversarial Fairness in Job Recommendation. In *RecSys in HR'22: The 2nd Workshop on Recommender Systems for Human Resources, in conjunction with the 16th ACM Conference on Recommender Systems*. https://arxiv.org/abs/2209.09592

[15] Manel Slokom, Alan Hanjalic, and Martha Larson. 2021. Towards user-oriented privacy for recommender system data: A personalization-based approach to gender obfuscation for user profiles. *Information Processing & Management* 58, 6 (2021), 102722. https://doi.org/10.1016/j.ipm.2021.102722

[16] Harald Steck. 2018. Calibrated recommendations. In *Proceedings of the 12th ACM Conference on Recommender Systems* (Vancouver, British Columbia, Canada) *(RecSys '18)*. Association for Computing Machinery, New York, NY, USA, 154–162. https://doi.org/10.1145/3240323.3240372

[17] Gonçalo Teixeira, Miguel Mira da Silva, and Ruben Pereira. 2019. The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance* 21 (06 2019). https://doi.org/10.1108/DPRG-01-2019-0007

[18] Tianhao Wang, Jeremiah Blocki, Ninghui Li, and Somesh Jha. 2017. Locally Differentially Private Protocols for Frequency Estimation. (08 2017).

[19] Tianhao Wang, Ninghui Li, and Somesh Jha. 2018. Locally Differentially Private Frequent Itemset Mining. *2018 IEEE Symposium on Security and Privacy (SP)* (2018), 127–143. https://api.semanticscholar.org/CorpusID:50787144

[20] Stanley L. Warner. 1965. Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias. *J. Amer. Statist. Assoc.* 60, 309 (1965), 63–69. arXiv:https://www.tandfonline.com/doi/pdf/10.1080/01621459.1965.10480775 https://www.tandfonline.com/doi/abs/10.1080/01621459.1965.10480775 PMID: 12261830.

[21] Yang Wu, Masayuki Mukunoki, Takuya Funatomi, Michihiko Minoh, and Shihong Lao. 2011. Optimizing Mean Reciprocal Rank for Person Re-identification. *2011 8th IEEE International Conference on Advanced Video and Signal-Based Surveillancei (AVSS)* (08 2011). https://doi.org/10.1109/AVSS.2011.6027363

[22] Zhenhuan Yang, Yingqiang Ge, Congzhe Su, Dingxian Wang, Xiaoting Zhao, and Yiming Ying. 2023. Fairness-aware Differentially Private Collaborative Filtering. In *Companion Proceedings of the ACM Web Conference 2023 (WWW '23, Vol. 32)*. ACM, 927–931. http://dx.doi.org/10.1145/3543873.3587577