Review 1	
Strengths:	-The paper proposes a novel privacy-aware transferable representation for cross-domain recommendation -The proposed approach is evaluated using three different datasets -The comparative evaluation using different recommendation approaches
Weaknesses:	- The connection to the Web conference should be made more explicit - When it comes to the envisaged transfer attack it is not clear from the text why a secure channel cannot be used - The authors assume a lot of background knowledge making the paper less accessible to non specialists
Summary and review comments:	The paper focuses on privacy preservation in the context of cross domain recommendations. The paper proposes a privacy-aware transferable representation, which can be used to improve recommendations in the target domain while at the same time protecting the private data from the source domain. The comparative evaluation confirms that the proposed PrNet recommendations are better than existing single domain models and have similar performance to existing cross domain models, while at the same time protecting the personal information from the source domain. Although I enjoyed reading the paper, I felt at times it was a little dense and could benefit from more concrete details, for instance some background/ preliminaries on: (i) the existing recommendation techniques presented in section 4.2.2, and (ii) adversarial learning technique in general. While the work is certainly relevant for online recommendation engines and thus would be of interest to the Web community, this connection should be better motivated in the paper. From a presentation perspective there are several grammatical issues that need to be fixed, for instance: - “the private information is not involved for improving recommendation” ->… not used for improving … - “CoNet learns a combination of two input activations and feed these combinations as input” -> … and feeds these …. -“ As shown in Eq. (3b), the party in the target network can access to the representations ...” -> … can access the representations …
Overall score:	**1**: (weak accept)
Review 2	
Strengths:	1. The motivation that learning privacy-aware transferable representations for users is very good, which could be helpful to real scenarios. 2. The paper is clearly written and the method is introduced in detail.

	3. The analysis of experimental results is reasonable.
Weaknesses:	1. The setting of the task in this paper is a bit strange. The ground-truth of user gender is calculated by another algorithm [39], and the proposed method tries to prevent other methods to predict user gender from the generated user feature. However, I have several questions. a. Is the algorithm [39] good enough to get the ground-truth? For example, if the accuracy of it [39] is 98%, the experimental results and conclusions in Table 2 and Table 3 may be different. b. According to the paper, attack algorithms have to get some ground-truths to train a model to recover the information behind user representations, how can they get them? c. It is much easier to collect user names than their feature embeddings and use the designed method [39] to predict user gender, attackers do not need to recover user gender from their representations. 2. In the experiment part, the introduction should be more detail. For example, why do the authors choose to combine two categories as one category in Section 4.1 but not use two of them? 3. About significant tests: a. From Table 3, the improvement of using the proposed privacy-aware method is marginal, which seems to be not significant. b. A significant test should be used in Table 2.
Summary and review comments:	This paper proposes to take user privacy into consideration when using cross-domain recommendations. The proposed defense model (PrNet) try to defense attacks with a new loss function, which is able to learn privacy-aware user representations. However, as pointed out in the Weaknesses part, the evaluation scenario is not good, and more analyses are necessary. Besides, there are too many typoes in the manuscript: a. In Abstract, the party in -> the part in b. In Section 1, see Fig. 2 -> see Fig. 1 c. In Section 3.1.2, can user any -> can use any d. In Section 3.1.2, see Fig. 2 -> see Fig. 1 e. In Table 2 and Table 3, x 100% -> x 100 ... In summary, the authors are encouraged to further improve their work.
Overall score:	**-2**: (reject)
Review 3	

Strengths:	The paper looks into the issue of privacy leakages in transfer learning, and uses a cross-domain adversarial learning to defend against these. The proposed metric proposed for leakage analysis is useful as the temporal aspect is taken into consideration. The use of the attacker simulation for optimization of the privacy loss is an interesting approach, though the proposed model is similar to GAN-based approaches recently proposed in a number of privacy-utility optimisation frameworks such as log-rank privacy. A number of datasets are used for the analysis.
Weaknesses:	Some of the known attacks have not been tried in the algorithm, like the known membership inferences attacks. Accuracy (precision) is calculated, but the recall and leakage information is not calculated. Privacy and utility tradeoff remains unclear
Summary and review comments:	While this paper touches upon an important topic, some of the aspects remain unresolved. The chosen metric for privacy versus accuracy is not fully developed to take into consideration membership inference attacks, and the figures in Fi (2) do not provide convincing results of the tradeoff. The attack improvements for different lambdas offered does not seem clear An important reference and attack model to consider here is the work in "L. Melis, C. Song, E. De Cristofaro, V. Shmatikov. Exploiting Unintended Feature Leakage in Collaborative Learning. S&P (Oakland) 2019." The accuracy values achieved are pretty low, would an accuracy of 50% be acceptable for a recommender system? It would have been great to put the focus of the paper on the metric, and assessing the layer-wise importance of the models used in transfer learning. I feel like given some time and effort, this would be a good paper, but it's not there yet. Some sentences need fixing, e.g., "Sometimes, it 67 may sacrifice a bit performance to protect privacy. "
Overall score:	**-2**: (reject)