Position Paper on Simulating Privacy Dynamics in Recommender Systems

PETER MÜLLNER, Know-Center Gmbh, Austria

ELISABETH LEX, Graz University of Technology, Austria

DOMINIK KOWALD, Know-Center Gmbh, Austria

In this position paper, we discuss the merits of simulating privacy dynamics in recommender systems. We study this issue at hand from two perspectives: Firstly, we present a conceptual approach to integrate privacy into recommender system simulations, whose key elements are *privacy agents*. These agents can enhance users' profiles with different privacy preferences, e.g., their inclination to disclose data to the recommender system. Plus, they can protect users' privacy by guarding all actions that could be a threat to privacy. For example, agents can prohibit a user's privacy-threatening actions or apply privacy-enhancing techniques, e.g., Differential Privacy, to make actions less threatening. Secondly, we identify three critical topics for future research in privacy-aware recommender system simulations: (i) *How could we model users' privacy preferences and protect users from performing any privacy-threatening actions?* (ii) *To what extent do privacy agents modify the users' document preferences?* (iii) *How do privacy preferences and privacy protections impact recommendations and privacy of others?* Our conceptual privacy-aware simulation approach makes it possible to investigate the impact of privacy preferences and privacy protection on the micro-level, i.e., a single user, but also on the macro-level, i.e., all recommender system users. With this work, we hope to present perspectives on how privacy-aware simulations could be realized, such that they enable researchers to study the dynamics of privacy within a recommender system.

1 INTRODUCTION

Through the increasing interest in novel evaluation methods for state-of-the-art recommender systems, research recognized that monitoring a recommender system from a static point of view is often not optimal. As an alternative, observing the dynamics of a recommender system via simulations showed its merit. However, modeling the complex and dynamic processes within a recommender system requires lots of engineering efforts. Hence, several popular simulation frameworks for recommender systems exist [1, 7]. In particular, simulations are beneficial for tracking any kind of effect within a recommender system. In this regard, recent simulation studies focus on, e.g., the evolution of popularity bias and feedback loops [8, 14], or the confounding of user behavior [2, 10].

In this paper, we present a modified simulation scheme for privacy-aware simulations, which makes it possible to discover the dynamics of privacy within a recommender system. Specifically, we propose *privacy agents* that enhance existing simulations with the ability to model privacy preferences and protect the privacy of users in a recommender system. A privacy agent bridges the gap between a user's preference model [15] and the user's privacy model [6, 12], and this way, the privacy agent serves two purposes. Firstly, it models a user's privacy preferences, e.g., a user's decision to disclose only certain information to the recommender system. Secondly, it protects a user from leaking sensitive

Authors' addresses: Peter Müllner, pmuellner@know-center.at, Know-Center Gmbh, Graz, Austria; Elisabeth Lex, elisabeth.lex@tugraz.at, Graz University of Technology, Graz, Austria; Dominik Kowald, dkowald@know-center.at, Know-Center Gmbh, Graz, Austria.

information by guarding the user's interactions with the recommender system. For example, when a user selects documents from the recommendation list and gives feedback to the recommender system, sensitive information could get leaked [13]. Typically, users have only minor knowledge of privacy threats and are unaware of privacy-enhancing techniques suitable to protect their privacy. Here, privacy agents provide a remedy, since they intervene and apply state-of-the-art privacy-enhancing techniques, e.g., Encryption [5] or Differential Privacy [3], to protect users from performing any privacy-threatening actions.

Moreover, we state three important issues, that are – as we think – crucial for designing privacy-aware recommender system simulations through privacy agents. Specifically, we briefly discuss (i) how adequate privacy agents could be developed, (ii) to what extent the privacy agents impact users' preferences and thus, drift from reality, and (iii) how one user's privacy agent could positively or negatively influence the recommendations and privacy of other users.

We think that similar to effects like, e.g., popularity bias, also privacy should not only be studied from a static point of view but by monitoring its dynamics in a recommender system. Thus, with our conceptual privacy-aware recommender system simulation approach presented in this position paper, we aim to give a future perspective on how the important aspect of privacy could be simulated. We hope that privacy-aware simulations complement insights gained by static evaluations and reveal interesting dynamics of users' privacy within a recommender system.

2   CURRENT PERSPECTIVE: PRIVACY-AGNOSTIC SIMULATIONS

Over the last years, a plethora of research emerged that simulates users and their interactions with a recommender system to grasp the dynamic nature of such systems. Issues to which recommender system simulations have been applied to include studying effects like item coverage or feedback loops, and analyzing the evolution of user preferences.

In particular, [4, 9] show that recommender systems tend to focus on a small set of documents when generating recommendations. This means that the evolution of the recommender system causes fewer documents to be covered. Plus, [9] provides a theoretical framework to model the recommender system's iterative behavior to investigate the presence of different biases. In the same vein, [14] analyze the emergence of popularity bias via recommender system simulations. In particular, the authors discuss the effect of different choice models and the kind of feedback users give to the recommender system on the emergence of popularity bias. In addition to feedback loops, [8] study filter bubbles and shed light on their effects on the dynamics of user interests. In summary, recent research utilized recommender system simulations to cover topics like popularity bias, feedback loops, filter bubbles, item discovery, and the evolution of user preferences. However, we highlight that research works – to the best of our knowledge – only use privacy-agnostic simulations.

A schematic overview of such a privacy-agnostic recommender system simulator is given in Figure 1, which is motivated by [7]. In the *Document Database*, all documents that are available for recommendation are stored. Each user is described by an individual *User Model*, which includes the user's document preferences and rating data. This is slightly different from the *Observable User Model*, which represents the recommender system's model of the user. Thus, this is the recommender system's knowledge about the user, which is a subset of the User Model. The *User Choice Model* defines how the user selects documents from the recommended list. For example, some users could seek serendipitous or novel recommendations, while other users would select documents based on familiarity. Depending on the received recommendations, users may change their interest in a certain direction and thus, shift the trajectory of the simulation. Thus, the *User Transition Matrix* measures how a user's preferences change over time. Finally, the *Recommender System Agent* generates a *Recommendation List* and receives the user's *Feedback*.
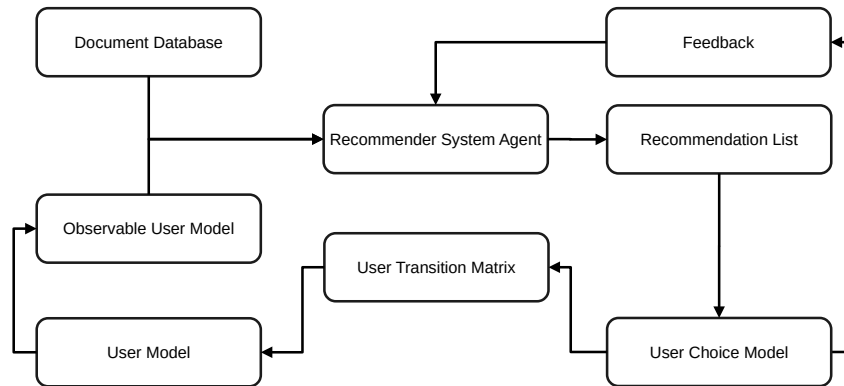
Fig. 1. Scheme of a typical privacy-agnostic recommender system simulator (motivated by [7]). The Recommender System Agent generates a Recommendation List from documents within the Document Database, based on its knowledge (i.e., Observable User Model) about a user (i.e., User Model). Then, the user chooses documents from the Recommendation List via a User Choice Model and gives Feedback to the Recommender System Agent. Plus, the documents chosen from the Recommendation List could lead to transitions in the User Model (i.e., User Transition Matrix).

Open Issue. Despite their recent popularity, privacy-agnostic simulations miss the important concept of privacy. For example, they are unaware of users' concerns and preferences regarding privacy. Furthermore, the effects of privacy protection, e.g., not disclosing data to the recommender system, are only studied in a static setting [11]. Similar to other factors, we believe that also privacy should be studied from a dynamic perspective. Hence, privacy-aware simulations are necessary to shed light on the dynamics of users' privacy within a recommender system.

3 FUTURE PERSPECTIVE: PRIVACY-AWARE SIMULATIONS

In this work, we propose privacy agents that enhance the existing recommender system simulation scheme in Figure 1 by incorporating users' privacy preferences and privacy protections, and thus, enable privacy-aware simulations. As illustrated in Figure 2, each privacy agent attaches to one user's User Model to (i) model what and how much data the user discloses (i.e., privacy preferences), or (ii) protects the user's privacy by guarding what and how much data is disclosed (i.e., privacy protection). Furthermore, the privacy agent also attaches to the User Choice Model and (i) models how the user selects documents in line with its privacy concerns (i.e., privacy preferences) or (ii) prohibits the user from selecting documents that would reveal sensitive information (i.e., privacy protection).

Privacy Agent. Firstly, it models a user's privacy preferences, e.g., not disclosing all data to the recommender system. Secondly, it protects a user's privacy by proposing what data to share and how documents to select from the Recommendation List to not compromise privacy. For example, the privacy agent could not only model a user's inclination to disclose data to the recommender system but also apply privacy-enhancing techniques to parts of the data, e.g., Encryption [5] or Differential Privacy [3]. In summary, the privacy agent can model users' privacy preferences and, additionally, can protect users from performing actions that would increase the risk of a privacy breach.

Open Research Questions. With our proposed privacy-aware recommender system simulation scheme, we aim to incorporate privacy to enable more realistic simulations. However, through the introduction of privacy-aware
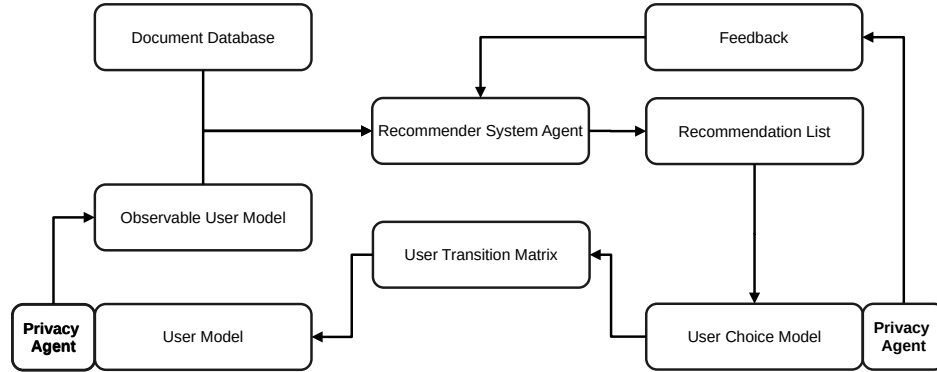
Fig. 2. Our proposed scheme of a privacy-aware recommender system simulator. Sensitive data about the user (i.e., User Model) could get leaked through the information available to the recommender system (i.e., Observable User Model) and the user's selection from the Recommendation List as defined by the User Choice Model. We introduce a privacy agent that attaches itself to the User Model and the User Choice Model to (i) model privacy preferences, or (ii) protect privacy.

simulations, several open research questions arise. Specifically, we highlight three questions that we think are of strong relevance, and thus, worth discussing among researchers.

(1) *How could we develop privacy agents that model users' privacy preferences, and protect users from performing any privacy-threatening actions?* To model users' privacy preferences, one could rely on questionnaires or construct artificial privacy models to model users with different privacy preferences. An additional question is how the privacy agents should decide on how to protect users' privacy. In detail, the agents could measure the privacy threat of users' actions by considering the users' privacy preferences but also by measuring the actions' danger from different perspectives (an actions' danger could change depending on the attack scenario), and then apply a suitable privacy-enhancing technique, e.g., Differential Privacy [3], Encryption [5], or data retention.

(2) *To what extent do the privacy agents modify the trajectory of the recommender system? This means, how are users' preferences manipulated when improving privacy?* Privacy agents could protect privacy by manipulating the user data available to the recommender system or by manipulating the way the user selects documents from the Recommendation List. Since the recommender system relies on these user interactions, the privacy agents influence what recommendations are generated. The recommendations can substantially influence users' preferences [14], and thus, it follows that protecting privacy by introducing privacy agents could also influence the User Models. Therefore, we think it is important to discuss to what extent the privacy agents' impact the User Models and how this could be prohibited.

(3) *How does modeling and protecting a user's privacy impact the recommendation quality and privacy of other users in the recommender system?* When a privacy agent intervenes to protect a user's privacy, a collaborative recommender system receives less-quality data from this user, which impacts the recommendations of other users within the system. This could lead to other users being pushed to disclose more about themselves to receive high-quality recommendations. Therefore, (i) monitoring the consequences of users' privacy agents, and (ii) making users aware of the consequences on other users seem to be two interesting aspects worth studying.

4 CONCLUSION & OUTLOOK

In this position paper at hand, we presented our perspective on privacy-aware recommender system simulations to study privacy in recommender systems from a dynamic point of view. In particular, we proposed to enhance existing privacy-agnostic simulation schemes by adding a privacy agent for each user. Firstly, the privacy agents model users' privacy preferences, e.g., their inclination to disclose data to the recommender system. Secondly, they guard users' interactions with the recommender system and apply privacy-enhancing techniques to protect users from leaking sensitive data through making privacy-threatening actions. Moreover, we discussed open research questions that are, in our opinion, strongly relevant for establishing privacy-aware simulations via privacy agents.

For future research, we suggest testing our privacy-aware simulation scheme by incorporating privacy agents into different simulation frameworks. Furthermore, in analogy to users collaboratively generating recommendations, we propose to research how privacy agents could collaborate to increase recommendation quality and privacy of all users simultaneously (i.e., optimize the privacy-accuracy trade-off).

REFERENCES

[1] Dimitrios Bountouridis, Jaron Harambam, Mykola Makhortykh, Mónica Marrero, Nava Tintarev, and Claudia Hauff. 2019. SIREN: A simulation framework for understanding the effects of recommender systems in online news environments. In *Proceedings of the conference on fairness, accountability, and transparency.* 150–159.

[2] Allison JB Chaney, Brandon M Stewart, and Barbara E Engelhardt. 2018. How algorithmic confounding in recommendation systems increases homogeneity and decreases utility. In *Proceedings of the 12th ACM Conference on Recommender Systems.* 224–232.

[3] Cynthia Dwork, Aaron Roth, et al. 2014. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science* 9, 3-4 (2014), 211–407.

[4] Andres Ferraro, Dietmar Jannach, and Xavier Serra. 2020. Exploring longitudinal effects of session-based recommendations. In *Fourteenth ACM Conference on Recommender Systems.* 474–479.

[5] Craig Gentry et al. 2009. *A fully homomorphic encryption scheme.* Vol. 20. Stanford university Stanford.

[6] Paul Grace and Mike Surridge. 2017. Towards a model of user-centered privacy preservation. In *Proceedings of the 12th International Conference on Availability, Reliability and Security.* 1–8.

[7] Eugene Ie, Chih wei Hsu, Martin Mladenov, Vihan Jain, Sanmit Narvekar, Jing Wang, Rui Wu, and Craig Boutilier. 2019. RecSim: A Configurable Simulation Platform for Recommender Systems. (2019). arXiv:1909.04847 [cs.LG]

[8] Ray Jiang, Silvia Chiappa, Tor Lattimore, András György, and Pushmeet Kohli. 2019. Degenerate feedback loops in recommender systems. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society.* 383–390.

[9] Sami Khenissi, Boujelbene Mariem, and Olfa Nasraoui. 2020. Theoretical Modeling of the Iterative Properties of User Discovery in a Collaborative Filtering Recommender System. In *Fourteenth ACM Conference on Recommender Systems.* 348–357.

[10] Masoud Mansoury, Himan Abdollahpouri, Mykola Pechenizkiy, Bamshad Mobasher, and Robin Burke. 2020. Feedback loop and bias amplification in recommender systems. In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management.* 2145–2148.

[11] Peter Muellner, Dominik Kowald, and Elisabeth Lex. 2021. Robustness of Meta Matrix Factorization Against Strict Privacy Constraints. In *Advances in Information Retrieval.* Springer International Publishing, Cham, 107–119.

[12] Vaikkunth Mugunthan, Anton Peraire-Bueno, and Lalana Kagal. 2020. PrivacyFL: A simulator for privacy-preserving and secure federated learning. In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management.* 3085–3092.

[13] Naren Ramakrishnan, Benjamin Keller, Batul Mirza, Ananth Grama, and George Karypis. 2002. When being Weak is Brave: Privacy Issues in Recommender Systems. *IEEE Internet Computing* (2002).

[14] Sirui Yao, Yoni Halpern, Nithum Thain, Xuezhi Wang, Kang Lee, Flavien Prost, Ed H Chi, Jilin Chen, and Alex Beutel. 2021. Measuring Recommender System Effects with Simulated Users. *arXiv preprint arXiv:2101.04526* (2021).

[15] Xiangyu Zhao, Long Xia, Lixin Zou, Dawei Yin, and Jiliang Tang. 2019. Toward simulating environments in reinforcement learning based recommendations. *arXiv preprint arXiv:1906.11462* (2019).