Proactively Control Privacy in Recommender Systems

ZIQIAN CHEN, Alibaba Group, China
FEI SUN, Alibaba Group, China
YIFAN TANG, Alibaba Group, China
HAOKUN CHEN, Alibaba Group, China
JINYANG GAO, Alibaba Group, China
BOLIN DING, Alibaba Group, United States

Recently, privacy issues in web services that rely on users’ personal data have raised great attention. Unlike existing privacy-preserving technologies such as federated learning and differential privacy, we explore another way to mitigate users’ privacy concerns, giving them control over their own data. For this goal, we propose a privacy aware recommendation framework that gives users delicate control over their personal data, including implicit behaviors, e.g., clicks and watches. In this new framework, users can proactively control which data to disclose based on the trade-off between anticipated privacy risks and potential utilities. Then we study users’ privacy decision making under different data disclosure mechanisms and recommendation models, and how their data disclosure decisions affect the recommender system’s performance.

To avoid the high cost of real-world experiments, we apply simulations to study the effects of our proposed framework. Specifically, we propose a reinforcement learning algorithm to simulate users’ decisions (with various sensitivities) under three proposed platform mechanisms on two datasets with three representative recommendation models. The simulation results show that the platform mechanisms with finer split granularity and more unrestrained disclosure strategy can bring better results for both end users and platforms than the “all or nothing” binary mechanism adopted by most real-world applications. It also shows that our proposed framework can effectively protect users’ privacy since they can obtain comparable or even better results with much less disclosed data.

CCS Concepts: • Information systems → Recommender systems; • Security and privacy → Privacy protections.

Additional Key Words and Phrases: Recommender System; Privacy; GDPR

ACM Reference Format:
Ziqian Chen, Fei Sun, Yifan Tang, Haokun Chen, Jinyang Gao, and Bolin Ding. 2022. Proactively Control Privacy in Recommender Systems. ACM Transactions on Information Systems 37, 4, Article 111 (August 2022), 21 pages. https://doi.org/X.XXXXX.XXXXXXX

1 INTRODUCTION

Recommender systems play an essential role on today’s web service platforms, e.g., e-commerce [45, 74] and social media [13, 78], since they can reduce users’ cognitive load by automatically offering...
personalized services that match their interests and needs [10]. While the recommender systems greatly facilitate the distribution and acquisition of information, they also bring critical privacy concerns due to unsolicited gathering users’ demographical and behavioral data [65, 81]. It has caused broad social effects. Several regulations have been proposed recently to better protect personal data, e.g., General Data Protection Regulation (GDPR) in the European Union and the California Privacy Rights Act (CPRA) in the United States.

One way to address this issue is to develop a privacy-preserving recommender system that can make recommendations without knowing users’ raw data. Two emerging technologies for this problem are federated learning [44, 51, 53, 56] and differential privacy (DP) [3, 18, 49, 64]. However, recent works have shown that they currently still have some limitations in practical use, e.g., information leakage through gradients [42, 82] and performance decrease in DP based methods [15]. Besides, users’ privacy concerns are also closely associated with their trust in these algorithms [2, 14].

Another promising remedy is to give users control over their data closure to reduce their privacy concerns [9, 80]. It means that users can proactively decide whether to disclose their personal data or not, which is also compatible with the principles (e.g., data minimization and opt-out) in privacy regulations like GDPR. Currently, real-world applications usually provide an opt-in checkbox for users to take an affirmative action to disclose all their data to the service providers. Usually, if the users do not choose to consent, they will either not be able to continue using the applications or not be able to enjoy the personalized services.

This raises a question, is such an “all or nothing” binary mechanism the best choice? Obviously, some privacy sensitive users might choose not to disclose their data. In this case, the user can not enjoy the benefits of personalized services. At the same time, the platform can not obtain revenue from these privacy sensitive users and also loses their data to train a better model. It seems that such a strict mechanism might not be a good choice for both parties in the ecology. So, is there a better mechanism that can reduce users’ privacy concerns and take into account the revenues of the platforms?

This paper aims to study how different privacy mechanisms affect users’ decisions on information disclosure and how their decisions affect the recommendation model’s performance and the platform’s revenue. For this purpose, we propose a privacy aware recommendation framework under privacy calculus theory [14, 40]. Under this new setting, users need to calculate the trade-off between the anticipated privacy risks and the potential utilities, then proactively control which data to disclose. In this way, all users’ dispersed privacy preferences are fully accommodated.

For service providers, they naturally want to entice users to disclose as much data as possible. For end users, they want to figure out how to enjoy the benefits of personalized services with minimal privacy risks. Formally speaking, under this privacy aware recommendation task setting, we aim to study what will happen if the platforms give users fine-grained control over their personal data. More specifically, we investigate questions including:

i) How do different platform mechanisms affect users’ decisions in information disclosure? Is the “all or nothing” binary mechanism the best choice for the platform?

ii) How do different recommendation models affect users’ decisions in information disclosure? Can a platform attract users to disclose more data by optimizing the model to provide better services?

To answer these questions, we first formulate our idea in formal settings. Following current researches in economics [43, 68], we model the privacy cost as a linear summation of the user’s disclosed personal data, meaning that the user loses control over such disclosed data, which also fits a fundamental notion in privacy calculus, i.e., the control over the data. Then recommendation
performance (e.g., NDCG) is employed as the potential utility from users’ disclosed data. To formally define user privacy decisions, we formulate the platform mechanisms using two components, i.e., data split rule and data disclosure choice space, which define the choices a user can take. Based on these simplified settings, we now can conduct experiments with different platform mechanisms or recommendation models to find answers to the above questions.

However, there is one big challenge for directly realizing our idea in real-world applications. Direct deployment of the proposed framework in real-world applications might seriously harm the end users’ experiences and the revenue of platforms. To address this challenge, inspired by the success of simulation studies in recommender systems [25, 38, 46, 76], we propose to use simulations to study the effects of the proposed framework. Specifically, we propose a reinforcement learning method to simulate users’ privacy decision making on two benchmark datasets with three representative recommendation models and three user types (i.e., different privacy sensitivity). The experimental results show that the platform mechanism with finer split granularity and more unconstrained disclosure strategy can bring better results for both end users and platforms than “all or nothing” binary mechanism adopted by most platforms. In addition to mechanism design, the results also point out that optimizing model is another option for the platform to collect more data while protecting user privacy.

Our main contributions can be summarized as following:

• We propose a privacy aware recommendation framework that gives users control over their personal data. To the best of our knowledge, this is the first work to give users fine-grained control over implicit feedback data in recommendation.
• We formulate the process of users’ privacy decision making and the platform’s data disclosure mechanisms using mathematics language. Then we instantiate the platform’s mechanisms with one data split rule and three data disclosure strategies that we proposed.
• We propose a reinforcement learning method to simulate users’ privacy decision making. The extensive simulations are conducted on two benchmark datasets with three representative recommendation models.
• The extensive experimental results show the effectiveness of our proposed framework in protecting users’ privacy. The results also shed some light on data disclosure mechanism design and model optimization.

2 FRAMEWORK FORMULATION

2.1 Overview

To mitigate users’ privacy concerns and comply with recent personal data protection regulations (e.g., GDPR)\(^1\), we proposed a privacy aware recommendation framework where users can freely choose which data to disclose with the recommender system. As illustrated in Fig. 1, the critical difference between our framework and traditional recommendation is that the platform can only use the sub-data disclosed by the users. For example, the user on the left in Fig. 1b can choose to hide his sensitive demographic attributes (e.g., age, gender, and education) and only discloses the last behavior to the service provider.

To enjoy the benefits of personalized services, users need to disclose their data to the recommender system to better model them. Intuitively, more data the recommender system gets, better results the users can get. However, disclosing data to the platform will increase users’ privacy concerns, e.g., data abusing [48] and privacy leakage [81]. Thus, under the privacy aware setting, users need

\(^1\)Although regulations, like GDPR, do not directly stipulate that platforms must provide the functions described in this paper, users can still achieve the same results through other legal rights like “the right to be forgotten”.

ACM Transactions on Information Systems, Vol. 37, No. 4, Article 111. Publication date: August 2022.
to make information disclosure decisions based on the trade-off between anticipated privacy risks and potential utilities. This idea can date back to *Privacy Calculus Theory* [14, 40].

Before going into details, we first define the entire personal data $\mathcal{D}_i$ of user $i \in \mathcal{V}$ as:

$$\mathcal{D}_i = \{ \mathcal{D}_{i,a}, \mathcal{D}_{i,b} \} = \{ a_{i1}, \ldots, a_{iK}, b_{i1}, \ldots, b_{it} \},$$  

(1)

where $\mathcal{D}_{i,a} = \{ a_{i1}, \ldots, a_{iK} \}$ denotes all user $i$’s profile attributes, $a_{ik}$ denotes the $k$-th profile attribute for user $i$, and $K$ is the number of profile attributes. $\mathcal{D}_{i,b} = \{ b_{i1}, \ldots, b_{it} \}$ denotes user $i$’s behaviors, $b_{ij}$ is the $j$-th behavior of user $i$, and $t_i$ is the last behavior timestamp.

A rational user is only willing to disclose data when she feels that she gains more from the platform than she loses in data disclosure. Formally speaking, supposing user $i$ with whole data $\mathcal{D}_i$ currently discloses data $\mathcal{S}_i \subset \mathcal{D}_i$, now she tries to get a better recommendation results via disclosing more data $\mathcal{S}_i' \subset \mathcal{D}_i$, where $|\mathcal{S}_i'| > |\mathcal{S}_i|$, only if

$$U_i(\mathcal{S}_i') - U_i(\mathcal{S}_i) > \lambda_i (C_i(\mathcal{S}_i') - C_i(\mathcal{S}_i)),$$  

(2)

where $U_i(x)$ denotes the utility that user $i$ can get from the platform with disclosed data $x$, function $C_i(x)$ measures the privacy cost paid by the user $i$ when she discloses the data $x$ to the platform, and $\lambda_i$ is the sensitive weight measuring how much user $i$ cares about her privacy. Apparently, compared to privacy insensitive users (i.e., small $\lambda_i$), the platform needs to provide more performance improvements to attract privacy sensitive users (i.e., large $\lambda_i$) to disclose their data. More details can be found in Section 3.3.2.

**2.1.1 **User Objective. Unlike traditional task settings where users can only passively accept recommendation results (i.e., without tools to optimize their objectives), in our framework, a rational user $i$ tends to maximize her utility $U_i(\mathcal{S}_i)$ while minimize the privacy risk $C_i(\mathcal{S}_i)$ by control the disclosed data $\mathcal{S}_i$. The objective function for a specific user $i$ can be formalized as the following for:

$$R_i(\mathcal{S}_i) = -\lambda_i C_i(\mathcal{S}_i) + U_i(\mathcal{S}_i).$$  

(3)

This formulation is also compatible with privacy related research in economics [17, 30, 43]. They studied the micro-foundation on a user’s intrinsic and instrumental preferences from disclosing personal information. In our formulation, user’s privacy cost $C_i(\mathcal{S}_i)$ corresponds to intrinsic value for personal data (i.e., protecting the data from being obtained by others), while recommendation utility $U_i(\mathcal{S}_i)$ corresponds to the instrumental value for personal data.
2.1.2 Platform Objective. In the proposed framework, the goal of a platform is still to maximize its revenue (e.g., purchases, clicks, or watching time) by improving the users’ recommendation utility (e.g., providing more accurate results). Thus, we define its objective as the summation of all users’ recommendation utilities in Eq. (3):

\[ R_p = \sum_{i \in V} U_i(S_i). \] (4)

Considering the utility also depends on the recommendation model, the utility function \( U_i(x) \) can be further defined as:

\[ U_i(S_i) = U(S_i) = U'(S_i, M_S), \] (5)

where \( M_S : s_i \rightarrow l_i \) (\( l_i \) is recommendation results) is a recommendation model trained using all users’ disclosed data \( S = \{s_1, \ldots, s_{|V|}\} \) and \( U' \) represents detailed recommendation utility function. Here, without loss of generality, we assume that all users share the same utility function.

**Recommendation Utility Function.** As shown in Eq. (3) and Eq. (4), the recommendation utility \( U \) occurs in the objective functions of both end users and the platform. Here, we use the users’ satisfaction with the results produced by the recommendation model to measure its utility. Such satisfaction is usually quantified by the user’s interactions with the recommendation results, e.g., clicks, watches, and reads. Based on such feedbacks, we can calculate different quantitative metrics as the utility in our framework, e.g., hit ratio and normalized discounted cumulative gain (NDCG) [28]. In this paper, we choose NDCG as the utility function \( U \) for all users because of its widespread use [21, 32, 66].

In traditional recommendation task, the platform can optimize this objective by only optimizing the model \( M_S \) since \( S_i = D_i \) is a fixed, i.e., all users disclose their whole data. However, this premise is broken in our proposed framework, where the user’s disclosed data \( S_i \) is varying. Thus, in our new framework, platforms also seek to attract users to share more data in other ways besides optimizing models, such as platform mechanism design.

2.2 Platform Mechanism

As mentioned before, the disclosed data \( S_i \) lives at the heart of the framework. Ideally, user \( i \) can freely choose any data \( S_i \) to disclose with the platform, e.g., choosing any profile attribute \( a \) or behavior data \( b \) as shown in Fig. 1b. However, in practice, such a degree of freedom is difficult to achieve for two reasons. On the one hand, from the perspective of human-computer interaction, too fine granularity of disclosure choice (e.g., single behavior) can adversely hurt user experience [79]. On the other hand, although the privacy regulations ensure users the right to determine the use of their data, they do not stipulate how the service providers implement this function.

In practice, the platform usually designs some data disclosure mechanisms to provide the end users with several convenient options. Here, we formulate the platform mechanism \( G = \langle \delta, \Pi \rangle \) using two components, data split rule \( \delta \) and disclosure choice spaces \( \Pi \). The data split rule \( \delta \) is regarded as a function that reorganizes the original user data \( D_i \) using different granularity, and \( \Pi \) denotes the space of all possible choices the platform provides to the user. We illustrate a toy example in Fig. 2.

2.2.1 Data Split Rule. Since user data usually consists of two different data types (as in Eq. (1)), we defined \( \delta \) as:

\[ \delta(x) = \{\delta_a(D_{i,a}), \delta_b(D_{i,b})\}, \]
where $\delta_a$ and $\delta_b$ have similar forms that split the original data into several pieces according to the corresponding granularity and rules:

$$\{x_1, x_2, \ldots, x_n\} \xrightarrow{\delta_b} \{x'_1, x'_2, \ldots, x'_m\},$$

where $m \leq n$ and $x'_j$ is the candidate units for data disclosure. According to the segmentation rules, $x'_j$ can be several consecutive data points like $\{x_1, x_2, x_3\}$ or discontinuous random data like $\{x_5, x_{22}\}$.

$\delta_a$ aims to reorganize the user’s profile attributes. The common approach is to keep original granularity (i.e., user can freely disclose any subset of attributes) or take all attributes as a whole (i.e., disclose all attributes or not). Formally, it can be instantiated as:

$$\delta_a(D_{i,a}) = \{a_{i1}, \ldots, a_{iK}\} \text{ or } \{\{a_{i1}, \ldots, a_{iK}\}\}. $$

Similarly, $\delta_b$ aims to transfer a user’s original behavior data (e.g., thousands of clicks or more views) to few data disclosure options. For example, "percentage split" with 10% granularity divides a user’s behavior sequence into 10 equal length subsequences, while "daily split" divides the user’s behaviors by day. Take “percentage split" with 10% granularity as an example, it can be instantiated as:

$$\delta_b(D_{i,b}) = \{s_{i,b1}, s_{i,b2}, \ldots, s_{i,b10}\},$$

where $S_{i,bj} = \{b_{i,[0,10]j}, b_{i,[1,10]j+1}, \ldots, b_{i,[10,10]j}\}$ is the $j$-th candidate option of behavior data for user to disclosed.

### 2.2.2 Data Disclosure Choice Space $\Pi$. Assuming the platform has transferred user $i$’s original data $D_i$ to $\delta(D_i) = \{s_{i,\omega_1}, \ldots, s_{i,\omega_n}, s_{i,\omega_{n+1}}, \ldots, s_{i,\omega_m}\}$, the platform can define data disclosure choice space $\Pi$ on these $m+n$ candidates as:

$$\Pi = \{\Pi_1, \Pi_2, \ldots, \Pi_N\},$$

$$\Pi_j \sim [0_1, \ldots, 0_k, \ldots, 0_{n+m}], \quad 0_k \in \{0, 1\},$$

where $0_k = 1$ denotes disclosing the $k$-th data in $\delta(D_i)$, while $0_k = 0$ means not; $\Pi_j$ is $j$-th data disclosure option that users can take; $N$ is the number of possible choices the platform provides to users. For example, a full 0 vector $\Pi_j = [0, 0, \ldots, 0]$ denotes that users can choose it to do not disclose any data. More detailed instantiations can be found in Section 3.2.

### 2.2.3 Platform Mechanism Design. With mechanism $G = <\delta, \Pi, >$, we can formally define the disclosed data $S_i$ from user $i$. Assuming user $i$’s original data $D_i$ has been spited into candidates $\delta(D_i) = \{s_{i,\omega_1}, \ldots, s_{i,\omega_m}\}$. Then, $S_i$ can be defined as the union of candidates in $\delta(D_i)$ selected by a specific choice $\alpha_i = \Pi_j \in \Pi$:

$$S_i = \alpha_i \otimes \delta(D_i) = \left\{ \bigcup_{\omega_i \in \delta(D_i)} S_{i,\omega_i} \right\},$$

where $\delta$ is the platform data split rule and action $\alpha_i$ is sampled from user $i$’s privacy disclosure policy $\pi_i$, which decides the data to be disclosed. The operator $\otimes$ denotes the aggregation of the selected split data based on his choice $\alpha_i$. Fig. 2 illustrates a tiny example of the data disclosure process (i.e., generation process of $S_i$) of a user with three profile attributes and four behaviors.

With formal definition of $S_i$, we can re-write the platform utility $R_p$ in Eq. (4) using platform mechanism $G$ and model $M_S$ as below,

$$R_p|_{G=\delta, \Pi,}\sum_{i \in V} U'_i(S_i, M_S) = \sum_{i \in V} U'_i(\alpha_i \otimes \delta(D_i), M_S).$$

---

2Here, we simplify the subscripts for easy description.
Fig. 2. An illustrative example for platform mechanism. The platform firstly split the user’s data \( \mathcal{D}_i \) (three profile attributes and four behaviors) using the rule \( \delta \) (keeping independent for attributes; percentage split with 50% granularity for behaviors). Then it provides choices \( \Pi_f \) for the user to choose to produce the final disclosed data \( S_i \).

One may figure out some possible optimal solutions towards the platform’s best mechanisms. However, the optimal platform mechanism design is another complex topic, usually considered from the view of game theory, and is out of scopes of this work. Here, we take the first step, studying the data disclosure decision of users and platform revenues under several common mechanisms.

3 SIMULATION

The most efficient way to figure out the answers to the questions we posed in the introduction is to deploy the proposed framework on a real-world platform and analyze how users adopt different and complex privacy policies to optimize their rewards. However, direct deployment of these strategies might seriously harm the end users’ experience and the platforms’ revenue. Moreover, researchers in academia also do not have the resources to deploy such experiments. Inspired by the success of simulation study on dynamic interactive problems in real-world applications [25, 38, 46, 76], we employ the simulation to study the effects of the proposed framework and the possible game between users and the platform.

3.1 Simplified Assumptions

To simplify the simulation process for easier analysis, we make some necessary assumptions to simplify the problem.

**Assumption 1 (Static Assumption).** User \( i \) optimizes her/his policy on the fixed data \( \mathcal{D}_i \) which is not affected by user policy \( \pi_i \).

Here static means the user data \( \mathcal{D}_i \) is fixed during the simulation, but the disclosed data \( S_i \) produced by different user policies is dynamic. It is also the most common setting for recommendation task in research papers [21, 24, 32, 59, 66]. In the simulation, we train the recommendation system \( M_S \) on the collected dynamic data \( \mathcal{S} \) and validate the recommendation efficiency on a fixed test set. In real-world applications, the data \( \mathcal{D}_i \), which contains the behavior data from the interaction with the recommender \( M_S \), is also dynamically changing with the user’s policy \( \pi_i \). It is beyond the scope of this paper and we leave it as the future work.
Assumption 2 (Immediate Assumption). The recommendation model $M_S$ can only use the data $S_i$ currently disclosed by each user $i$.

The motivation of this assumption is that an untrusted platform can leverage user $i$’s all data $D_i$ if it can use the data disclosed in previous actions. Without this constraint, the privacy right discussed in this paper is meaningless. To achieve this, the platform can retrain the model from scratch with new data $S'_i$ or quick unlearn the data in $S_i$ then finetune with data $S'_i$ [5, 6, 8].

However, the Assumption 2 also raises a new challenge that the asynchronous changes of user policy bring intractable computation costs for the platform since each time the user changes the disclosed data, the platform needs to update the model. Here, we make an assumption for simplifying the simulation, assuming all users realize that the platform will cyclically (e.g., once a day) collect their privacy decisions and update recommender systems.

Assumption 3 (Cyclical Assumption). Platform cyclically collects user privacy choices, and then the platform updates the model using all newly disclosed data.

In summary, for easy analysis in simulations, we introduce these assumptions to ignore the time and dynamic effects in this feedback system, just like the traditional recommendation task formulation.

3.2 Platform Mechanism Simulation

In order to validate the effect of the platform mechanism, we adopt several mechanisms during simulation. For easy comparison, we utilize one mechanism at each experiment.

Data Split Rule. In our simulation, we keep the original granularity towards user profile attributes, where the user can freely determine whether to share any subset of their attributes.

For behavior data, we apply “percentage split” as $\delta_b$ with different split granularity $\rho$ (e.g., 1/3) to split the behavior sequence into $1/\rho$ parts. One obvious advantage of “percentage split” is that it can normalize the size of user action space and decrease the inconvenience of the interaction between the user and the platform.

Data Disclosure Strategy. As the platforms have certain flexibility to implement different data disclosure strategies, we discuss three representative disclosure strategies used in our study for behavior data in this subsection. These strategies determine the data disclosure action space $\Pi$ the user can choose. For profile attributes, we found that all users tend not to disclose them in the experiments since these features are negligible for improving recommendation utility in the presence of behavior data. Thus, in the following study, we mainly focus on modeling only behavior data.

The “separate” rule gives the users the control to freely disclose any split personal data. For this rule, the size of user $i$’s the action space is exponentially expended on the size of the spilt data set $|\delta_b(D_{i,b})|$, denoted as $2^{|\delta_b(D_{i,b})|}$. However, too many choices might make it difficult for users to make better data disclosure decisions.

Another data disclosure strategy named “oldest continuous” provides users the choices to disclose continuous behavior data from the beginning time, such as selecting “the oldest 33% data”. In this strategy, to disclose newer behavior data $S_{i,b,j}$, users must also disclose all behavior data before it. Take an already split data $\delta_b(D_{i,b}) = \{S_{i,b1}, S_{i,b2}, S_{i,b3}\}$ as an example, the action space provided by oldest continuous strategy is $\Pi = \{[0, 0, 0], [1, 0, 0], [1, 1, 0], [1, 1, 1]\}$, and its corresponding disclosed data is $\{\emptyset, \{S_{i,b1}\}, \{S_{i,b1}, S_{i,b2}\}, \{S_{i,b1}, S_{i,b2}, S_{i,b3}\}\}$. "Latest continuous" mechanism is similar to "oldest continuous", with the only difference in the opposite direction. The size of these two mechanisms’ action spaces is $|\delta_b(D_{i,b})|$. 

ACM Transactions on Information Systems, Vol. 37, No. 4, Article 111. Publication date: August 2022.
3.3 User Policy Simulation

In this subsection, we introduce the simulation of user policy in our proposed framework. As defined in Eq. (6), the disclosed data $S_i$ is result of the platform mechanism $G$ and user’s disclosure policy $\pi_i$. Meanwhile, in Eq. (5), the recommendation utility $U_i(S_i) = U'(S_i, M_S)$ is also determined by the recommendation model $M_S$, which is build upon the all users’ disclosed data $S$. The reward of user $i$ may be varied even when $i$ keeps the disclosed data $S_i$ unchanged since other users might change their disclosed data and the recommender system is changed. Thus, the expectation rewards are considered rather than immediate value defined in Eq. (3) and we assume all the users are rational and seek for the optimal privacy disclosure action $\alpha_i^*$ to the optimal expected reward $E[R_i|\alpha_i]$ as his policy, i.e.,

$$\alpha_i^* = \arg\max_{\alpha_i \in \Pi} E[R_i|\alpha_i] = \arg\max_{\alpha_i \in \Pi} E[R_i(S_i)]$$

$$= \arg\max_{\alpha_i \in \Pi} E[-\lambda_i C_i(\alpha_i \otimes \delta(D_i)) + U_i(\alpha_i \otimes \delta(D_i))].$$

(8)

As mentioned before, recommendation utility $U_i$ has been discussed in Section 2.1.2. To study this objective, we need to define the privacy cost function $C_i$ and sensitive weight $\lambda_i$.

3.3.1 Privacy Cost Function. We simulate every user with the same cost function $C$ and leave the diversity of user privacy sensitivity to the parameter $\lambda_i$. Following current experiment specifications in the economics literature [43, 68], we model the privacy cost function as a linear summation\(^3\) of disclosed personal data. As mentioned in Section 3.2, user tend not to disclose profile attributes $D_{i,a}$ due to no gains in our experiments, so we only consider behavior data here, i.e.,

$$C_i(S_i) = C(S_i) = |S_i|/|S_i|,$$

(9)

where the $|x|$ is the number of elements in $x$. Here, the percentage based measurement regards different amount of users’ data equally.

This reduced form specification is not unrealistic as it captures the substitution effect among personal data and incorporates the idea of constant marginal privacy cost. One might argue for a higher order functional to capture richer implications. However, there is little experimental evidence that the higher order form for privacy cost exists and how the functional form looks like.

3.3.2 Privacy Sensitive Weight. For user $i$ who disclosed all her/his data (i.e., $S_i = D_i$), her/his privacy cost compared to not sharing any data (i.e., $S_i = \emptyset$) is

$$C(D_i) - C(\emptyset).$$

(10)

Meanwhile, her/his anticipated recommendation utility compared to not sharing any data is:

$$U(D_i) - U(\emptyset).$$

(11)

We assume all users have accessed to the recommendation utility $U(D_i) = U'(D_i, M_p)$ computed on all the data $D_i$ and the recommendation utility without their data $U(\emptyset)$ before they can take data disclosing actions, which can be regard as a prior knowledge, like the experiences before the platform adopted our framework. With Eq. (10) and Eq. (11), we define the privacy sensitive weight $\lambda_i$ as:

$$\lambda_i = w_i * \frac{U(D_i) - U(\emptyset)}{C(D_i) - C(\emptyset)},$$

(12)

where $w_i$ indicates the diversity of user types towards privacy sensitivity. The users with $w_i > 1$ is privacy sensitive users, as they will not be willing to disclose the corresponding data $D_i$ if they only

\(^3\)See the Eq. 2 in [43] and the dis-utility from disclosure in the econometric specification session in [68].
get $U(\mathcal{D}_i)$ as before. While users with $w_i < 1$ are just the opposite. Therefore, the user’s privacy sensitive weight is pre-computed, and the $U(\mathcal{D}_i)$ can be regarded as the benchmark expectation of the platform. The formulation of the privacy sensitive weight $\lambda_i$ also meets the idea from [43], where the heterogeneity from users’ social demographic variety should also be explicitly characterized.

3.3.3 Simulation Algorithm. As users behave rationally to find the optimal strategy with a trade-off of exploration and exploitation, it just meets the idea of the reinforcement learning algorithm. Therefore, we model each user as a unique agent and apply a multi-agent reinforcement learning method to simulate user possible policy adaptation. The recommender system is regarded as the environment to provide feedback, which is build upon the disclosed user data. All agents’ policies are optimized simultaneously by determining their actions, i.e., the disclosed data $s'$ at simulation epoch $t$, which is used to train the recommendation model $M_{s'}$. As mentioned before, users tend to find an optimal action over possible action space $\Pi$ to maximize his expected reward, which is determined by all agents in this dynamic MARL environment.

We assume each user (agent) realizes this situation that the immediate reward is the result of the user’s policy $\pi_i$ as following,

$$
\alpha_i^{t+1} = \begin{cases} 
\alpha_i \sim P_i^t, & \text{with possibility } \epsilon \\
\arg\max_{\alpha_i} Q_i^t(\alpha_i), & \text{with possibility } 1 - \epsilon
\end{cases}
$$

(13)

where $Q_i^t(\alpha)$ is the user $i$’s estimation value at simulation epoch $t$ on action $\alpha$, and $P_i^t$ denotes a random sample policy. To conduct an efficient policy exploration, we sample a less explored action with a higher possibility as following,

$$
P_i^t(\alpha) = \frac{1/(N_i^{t-1}(\alpha) + 1)}{\sum_{x \in \Pi} 1/(N_i^{t-1}(x) + 1)},
$$

(14)

where $N_i^{t-1}(\alpha)$ represents the total number of action $\alpha$ was taken by user $i$ from start to the last simulation epoch $t-1$. In convenience, we adopt the approximated expected estimation results and update it with the residual between the estimation $Q_i^{t-1}(\alpha_i^{t-1})$ and immediate reward $R_i^{t-1}$ when she/he takes action $\alpha_i^{t-1}$ as following.

$$
Q_i^t(\alpha) = \begin{cases} 
Q_i^{t-1}(\alpha), & \text{if } \alpha_i^{t-1} \neq \alpha \\
Q_i^{t-1}(\alpha) + \frac{1}{N_i^{t}(\alpha)}(R_i^{t-1}(\alpha \otimes \delta(\mathcal{D}_i)) - Q_i^{t-1}(\alpha)), & \text{if } \alpha_i^{t-1} = \alpha
\end{cases}
$$

where $R_i^{t-1}$ is user $i$-th immediate objective at simulation epoch $t-1$, computed by Eq. (3). $Q_i^0(\alpha)$ is the user $i$’s initial expected reward if she/he takes action $\alpha$, which is initialized to 0 as users have no prior about their behaviors on the new dynamic environment.

In our simulation, we set initial $\epsilon = 0.5$ for all agents and decay a half during the MARL training processing. The detailed decay epoch is co-related to the size of possible action space $\Pi$. Here, we define it as $\epsilon = 0.5^{t/(3\times|\Pi|)}$, where $t$ is the epoch during the reinforcement learning training processing.
Table 1. Statistical details of the evaluation datasets.

| Dataset  | #User | #Item | #Interaction | Density     |
|----------|-------|-------|--------------|-------------|
| ML-100k  | 637   | 1278  | 90,554       | 11.1234%    |
| Yelp     | 8338  | 35,476| 760,635      | 0.2571%     |

4 EXPERIMENTS

4.1 Research Question

- RQ1: How do different platform mechanisms affect the recommendation performance and the data disclosure decisions of users with different privacy sensitivity?
- RQ2: What is the role of recommendation model in this framework? Can a more accurate model attract users to disclose more data?
- RQ3: How does user population composition affects the user behavior in this framework?

4.2 Experiment Setup

4.2.1 Dataset. We conduct our experiments on two real-world representative datasets which vary in domains and sparsity: MovieLens-100k⁴ (ML-100k) [19] and Yelp⁵. Since we focus on recommendation based on implicit feedback, we follow the common practice to convert the numeric rating or a review into implicit feedback of 1 (i.e., indicating the user interacted with the item). After that, we build the behavior sequence for each user by grouping and sorting their behaviors according to the timestamps. To properly simulate the information disclosure decision making process, we filter out the user with less than 40 interactions and items with less than 5 interactions. For efficiency reasons, we further subsample the users in Yelp, resulting in a dataset with 8338 users. The statistics of the processed datasets are summarized in Table 1.

4.2.2 Simulation Setup. For each user, we hold out the last item of the behavior data as the test data to compute recommendation utility [21, 32, 66]. The rest of the behavior data is used for training simulation, treating the last interaction data in disclosed data as validation data and the remaining disclosed data for training data.

For recommendation utility evaluation, we adopt the widely used leave-one-out evaluation [21, 32, 66] protocol with NDCG@100 computed on the whole item set as the metric. In particular, for Yelp, we compute the sampled metric with 1000 negative samples since the large item candidate set makes the results on Yelp are too small to simulate stably. These sampled results are consistent with the scores on the whole candidate set [39].

For privacy risk function, we use disclosed data percentage measurement according to Section 3.3.1, which is weighted by the sensitive weight λᵢ defined in Eq. (12). To study the data disclosure decision making for users with different privacy sensitivity, we randomly divide users into three groups (each with 1/3 users) with different privacy sensitive levels by adjusting the wᵢ,

- wᵢ = 0: non-sensitive user who does not care privacy at all.
- wᵢ = 1: normal user who weights privacy risk and recommendation results in a relatively normal way.
- wᵢ = 10: sensitive user who is more concerned about privacy.

⁴https://grouplens.org/datasets/movielens/100k/
⁵https://www.kaggle.com/yelp-dataset/yelp-dataset
To acquire the sensitive weight $\lambda_i$, the benchmark recommendation result $U(D_i)$ is computed based on GRU model with the whole dataset. The assumption here is that the non-privacy aware framework that the user used before was based on GRU4Rec.

In the RL training, we model each user as an agent following the setup, and train 400 epochs with Epsilon Greedy algorithm. In each simulation epoch, the recommendation model is trained from scratch as discussed in Assumption 2, i.e., the platform can only use the data that the user disclosed in the current simulation epoch. The simulation epoch is enlarged to 3000 epochs in “separate” data disclosure strategy with $p = 1/8$ due to the slow convergence.

4.2.3 Recommendation Model. To study the role of different models in users’ data disclosure decision making, we conduct the simulations on different models, including two state of the art sequential recommendation models (i.e, GRU4Rec [24] and BiSA (bidirectional self-attention) [32, 66]) and one CF model (i.e., NCF [21]).

We implement these models using PyTorch\(^6\). The hype-parameters are carefully tuned using a grid search to achieve optimal performances. After tuning, the embedding size and hidden size is set to 128 for all the models, the dropout ratio is set to 0.2, the learning rate equals to 1e-3 for the models except BiSA with a learning rate 3e-4, and the number of negative samples is set to 16. All models are trained with adam optimizer [34] with early stop.

4.3 Study 1: Impact of Platform Mechanism

We firstly conduct experiments on platform mechanisms specifying various data split granularity and data disclosure strategies with a widely-used sequential recommendation model GRU4Rec. We begin by answering which mechanism is preferred by users with different privacy sensitivity (types, hereafter).

4.3.1 Split Granularity $p$. We first validate how the split granularity affects users on the three aforementioned data disclosure strategies. The recommendation results and the data disclosure

---

\(6\) The source code will be released after the review phase.
percentage on different user types are reported in Table 2 where all results are averaged on the last 20 epochs after convergence. From the results, it can be observed that:

1. Comparing the NDCG performances among different settings, we can derive a negative answer for the question in the introduction considering “all or nothing” binary choice (i.e., $p=1$) performs worst on all disclosure strategies for all datasets. Even looking at the detailed results for user groups with different privacy sensitivity, $p=1$ still performs very poorly, if not the worst.

2. Comparing the results within different user groups, a prominent and expected result is that users who care about privacy are only willing to disclose very little data, especially privacy sensitive users. Besides, normal users can obtain comparable recommendation results (even better on ML-100k) to non-sensitive users with much less data. On the one hand, this indicates that our proposed framework can effectively protect users’ privacy. On the other hand, proactively controlling the disclosed data also allows users to improve their recommendation results by themselves.

3. For platform, finer split granularity can usually bring better performances in all three mechanisms for all datasets. Unexpectedly, these superior performances are not always obtained through more disclosed data. For example, under “latest continuous” rule, the overall recommendation performances for $p=1/16$ (16.31% on ML-100k) are much better than $p=1/2$ (13.89% on ML-100k) with less training data (40.45% vs. 43.57% on ML-100k).

To figure out the reason for this phenomenon, we analyzed the distribution of user’s data disclosure. We reported the percentage of users who disclosed data in Table 3. The results show that more users turn to disclose data since finer granularity allows users to disclose a small amount of data for certain recommendation utilities. Conversely, more users suffer from poor recommendations as they refuse to disclose data under coarse-grained granularity.

4.3.2 Data Disclosure Strategy. We study how data disclosure strategy affects users’ decisions using three strategies with different degrees of freedom. The results are also reported in Table 2.

It is easy to see that the flexible “separate” strategy is superior to other mechanisms within the same granularity. The “separate” strategy achieves better overall recommendation results with similar or even less disclosed data. One possible reason is that it enables users to freely disclose the data that benefits their recommendations. In this way, users will discard those data that are not helpful for their recommendations, which is equivalent to data optimization by users. It also explains why “separate” with $p=1/8$ outperforms “all” in ML-100K. These results are consistent with the research in data minimization [4, 11, 73].

For the other two strategies, i.e., “latest continuous” and “oldest continuous”, the results show they perform not very consistently in different datasets. This could be caused by the characteristics...
Fig. 3. Simulation process using “oldest continuous” strategy with different granularity \( p \) on ML-100k. The results are smoothed using exponential moving average with smoothing factor 0.9 for clearer visualization. The black line denotes the “separate” with \( p=1/8 \) on ML-100k truncated at 400 epochs.

Table 4. Results on different recommendation models with different platform mechanism. “dis.\%” denotes average user data disclosure percentage, “NDCG” means NDCG@100 (%). All the results are averaged on the last 20 epochs.

| strategy | model | ML-100k | Yelp |
|----------|-------|---------|------|
|          | non-sensitive | normal | sensitive | all | non-sensitive | normal | sensitive | all | non-sensitive | normal | sensitive | all | non-sensitive | normal | sensitive | all |
| latest cont. \( p=1/16 \) | NCF | 10.73 | 100 | 15.69 | 13.52 | 9.87 | 9.78 | 12.10 | 19.82 | 23.18 | 100 | 15.37 | 16.90 | 13.60 | 5.85 | 20.79 | 41.41 |
|          | GRU4Rec | 17.65 | 100 | 19.26 | 16.22 | 12.01 | 8.82 | 16.31 | 40.45 | 26.09 | 100 | 25.82 | 17.22 | 15.62 | 6.08 | 22.33 | 41.10 |
|          | BiSA | 18.04 | 100 | 21.86 | 15.61 | 14.55 | 12.80 | 18.16 | 40.44 | 25.35 | 100 | 26.31 | 12.85 | 19.48 | 7.14 | 23.72 | 40.38 |
| oldest cont. \( p=1/16 \) | NCF | 11.60 | 100 | 14.08 | 14.88 | 10.11 | 7.80 | 11.93 | 39.61 | 23.21 | 100 | 21.13 | 15.97 | 10.22 | 4.56 | 18.19 | 40.71 |
|          | GRU4Rec | 17.55 | 100 | 21.55 | 26.85 | 12.88 | 17.03 | 17.33 | 46.89 | 25.99 | 100 | 24.77 | 24.68 | 11.06 | 6.46 | 20.61 | 44.21 |
|          | BiSA | 18.05 | 100 | 24.52 | 34.72 | 18.32 | 15.73 | 18.64 | 49.85 | 25.16 | 100 | 31.53 | 26.03 | 14.97 | 8.66 | 23.72 | 45.18 |
| separate \( p=1/4 \) | NCF | 11.37 | 100 | 16.32 | 17.57 | 9.06 | 8.37 | 12.25 | 40.76 | 23.81 | 100 | 27.25 | 24.60 | 5.73 | 3.32 | 18.92 | 43.15 |
|          | GRU4Rec | 17.38 | 100 | 22.26 | 23.88 | 9.44 | 11.85 | 16.36 | 44.12 | 26.48 | 100 | 29.97 | 27.73 | 4.56 | 4.64 | 20.34 | 44.61 |
|          | BiSA | 17.33 | 100 | 24.33 | 25.40 | 9.64 | 12.42 | 17.17 | 45.42 | 26.30 | 100 | 28.47 | 26.32 | 6.64 | 5.92 | 21.14 | 44.28 |

of different datasets. It reminds us to design data disclosure mechanisms carefully according to the characteristics of data we deal with in real-world applications.

In summary, the platform mechanism affects both the possibility of a user to disclose and the volume of her/his disclosed data. Normally, a finer granularity and a more free data disclosure strategy can improve recommendation results for users and better protect users’ privacy at the same time. However, the price is that a large action space leads to slow convergence on the optimal user policy. As shown in Fig. 3, “separate” with \( p=1/8 \) (128 possible options) converges much slower than other mechanisms. It indicates users might be hard to find their best policies under these fine-grained mechanisms. Thus, we constraint users’ possible choice number to 16 for all mechanisms for fair comparisons in the latter experiments.

4.4 Study 2: Impact of Recommender

This study answers whether a better model (BiSA) or a worse model (NCF) will attract users to disclose more data or not. Table 4 reports the results on three different data disclosure strategies
Table 5. Results for different user group compositions on ML-100K. All the results are averaged on the last 20 epochs.

| Strategy   | NDCG@100 (%)          | Statistics of data disclosure (% of disclosed data (avg. # user)) |
|------------|-----------------------|---------------------------------------------------------------------|
|            | #100% Non-sen | #100% normal | #100 % sensitive | #1:1:1 |
| latest     | $p = 1/16$   | 19.45       | 16.64           | 10.50  | 16.31  |
| oldest     | $p = 1/16$   | 19.45       | 18.76           | 11.87  | 17.33  |
| separate   | $p = 1/4$    | 19.45       | 19.28           | 9.27   | 16.36  |

with optimal granularity $p = 1/16$ except the $p = 1/4$ on “separate” for keeping the same number of data disclosing choices. It can be observed that:

1) The results show that a more powerful model BiSA can attract sensitive users to disclose more data by improving the recommendation results for all platform mechanisms on all datasets. In contrast, the worse model NCF is the opposite. 2) Though a better model usually can incentive users to disclose data, the total volume of data disclosed by normal users is not always increased. One reason is that marginal recommendation utility by disclosing more data may decrease on a better model considering the model already predicted precisely based on the disclosed data. This phenomenon is prominent on the BiSA in “latest continuous” considering a better sequential model may rely less on older behavior data [32, 66].

In summary, the Table 4 results suggest that the platform may pay more attention towards mechanism optimization while always stick to a better recommender system.

4.5 Ablation Study

Here, we study the impacts of compositions of user groups and the privacy sensitive hyper-parameter $w_i$. Due to page limitation, we only report the results based on GRU4Rec on ML-100k.

4.5.1 User Group Compositions. In this subsection, we adjust the user group composition where each user in the dataset is non-sensitive/normal/sensitive. The average percentage of disclosed data and recommendation results are reported in Table 5. The platform can get higher revenues when users are less concerned about their privacy risks. Moreover, user group compositions play a more critical role in the platform’s revenue than the data disclosure mechanisms. This encourages the platform to take more actions on privacy protection to prevent users from becoming sensitive.

4.5.2 Privacy Sensitive. We report the effects of the hyper-parameter $w_i$ in Fig. 4. The results show that all mechanisms perform quite stable on both recommendation results and data disclosure with different hyper-parameter $w$, especially when $w > 5$. The reason for these results is that a user will barely disclose their data unless she/he observes a significant improvement on the recommendation results when her/his privacy sensitivity is very high (e.g., $w > 5$). This also demonstrates that the conclusions of our previous experiments are stable.
5 RELATED WORK

5.1 Recommendation Systems

Early works on recommender systems mainly model the users’ interests statically as collaborative filtering (CF) task with implicit feedback. Early representative works include item-base CF algorithms [45, 61] and matrix factorization (MF) [37, 52] Recently, deep learning has also revolutionized collaborative filtering. One line of research seeks to improve the CF models with the representation learned from auxiliary information, e.g., text [70] and images [72] using deep learning models. While more mainstream way is to take the place of conventional CF models with more powerful neural models, like neural collaborative filtering (NCF) [22] and graph neural network based recommendation models [20, 78].

In recent years, sequential recommendation has become another mainstream task in recommender systems since it can better capture users’ dynamic interests from their historical behaviors [57]. Sequential recommendation has also experienced the development process from traditional markov chain based models [59, 62] to neural sequential models, e.g., GRU4Rec [23, 24] and self-attention models [32, 66]. Considering that sequential recommendation has become the mainstream in real-world applications [41, 47], we study the new proposed task based on a sequential setting in this paper.

5.2 Privacy in Recommender Systems

The research about privacy concerns in recommender systems can be classified into two categories: privacy-preserving recommendation modeling and decision making in privacy.

Privacy-preserving recommendation modeling mainly aims to protect user’s sensitive information from being leaked by designing specific models. An emerging paradigm is to use federated learning to train recommender systems without uploading users’ data to the central server [44, 53, 56, 71]. Federated learning dramatically enhances user privacy since user data never leaves their devices. However, recent works have shown that federated learning can unintentionally leak information through gradients [42, 82] and is also vulnerable to attacks like membership inference attacks [50, 54]. To address such issues, differential privacy [16], a powerful mathematic framework for privacy, has been employed to guarantee user privacy in the procedure of recommender systems [3, 18, 49, 64]. The basic idea of this paradigm is to add random noise into the recommender

ACM Transactions on Information Systems, Vol. 37, No. 4, Article 111. Publication date: August 2022.
system to prevent information leakage. As a promising framework, one limitation of differential privacy is that it usually decreases performance [15].

**Decision making in privacy** from other disciplines, e.g., economic [43], management sciences [14], and human–computer interaction [35, 36], mainly focus on studying the problem like where privacy concerns come from and how to mitigate them. They mainly study the procedure of user’s decision making about information disclosure using the privacy calculus theory [14, 40], which views privacy as an economic commodity. It is to say that the user decides to disclose his/her information by weighing the anticipated risks of disclosing personal information against the perceived utility. Numerous works have studied the factors that influenced the user’s decision using questionnaires or mock-up applications [9, 35, 36, 79]. Multiple studies highlight that “control” is a key factor in decision making about privacy, and providing control over the recommendation process to users can reduce their privacy concerns [9, 80]. Going a step further, in this paper, we give users not only control over whether or not to disclose data, but also control over which data to disclose. Then we investigate the consequences caused by this novel setting, including how users make choices and how different platform mechanisms and recommendation models perform.

Another close work to ours is [75] that studies a recommendation task where a small set of “public” users who disclose all their ratings (large amount) and a large set of “private” users refuse to disclose their data. Our work differs from [75] in the following aspects: i) Most importantly, as explained in the introduction and last paragraph, our goal is not the performances of the recommender systems; ii) We provide users with more fine-grained control over their data; iii) our task is built on implicit feedback, which is the mainstream of the real-world applications.

### 5.3 Simulation

Recent years have witnessed the wide applications of the simulation techniques among various scenarios, e.g., recommendation [7, 27, 46, 77], autopilot [55], traffic scheduling [1, 12] and robotic [58]. The primary reason to utilize simulation is that straightforwardly conducting experiments in the real world may remain too expensive [63] and risky [55]. Besides, the solutions derived from simulations can be transferred to solve the real-world problems [63, 69].

In the research areas of recommender systems, it is of great significance to utilize the carefully designed simulation environments to efficiently evaluate recommendation policy [63] or draw insightful conclusions for specific studies such as societal impact analysis [7]. Ie et al. [26] builds upon a simulation environment for slate-based recommender systems, which facilitates the recommendation policy evaluation. Shi et al. [63] proposes to utilize the historical user behavior data to train the simulator and verifies that the policies trained in the simulator achieve superior online performance. A series of works [7, 46, 77] utilize simulation environments to get in touch with user society impacts over recommender systems such as fairness and societal biases.

There also exist a series of works to simulate user decisions to maximize their personalized utilities [29, 31, 60]. Typically, the user is modeled as a rational agent whose policy can be learned following a trial-and-error schema such as RL-based algorithms [31, 33]. In this work, each user is modeled as a rational agent to optimize his (her) unique data disclosure policy under a designed platform mechanism. The efficiency of recommender systems is also evaluated within such a simulation environment.

### 6 CONCLUSIONS AND FUTURE WORK

This paper proposes a privacy aware recommendation framework based on privacy calculus theory to study what will happen if the platform gives users control over their personal data. To avoid the great cost in online experiments, we propose to use reinforcement learning to simulate the users’ privacy decision making under different platform mechanisms and recommendation models.
on public benchmark datasets. The results show a well-designed data disclosure mechanism can perform much better than the popular “all or nothing” binary mechanism. Our work provides some insights to improve current rough solutions in privacy protection regulations, e.g., opt-in under GDPR and opt-out under CCPA.

This paper only takes the first step in giving user privacy control over the recommender systems, and several directions remain to be explored. First, a more complex and accurate privacy cost function can help us better understand users’ privacy decision making. Second, more sophisticated platform mechanisms are also worth exploring. Last but not least, deploying online experiments and analyzing users’ decisions in real-world can facilitate further research.

REFERENCES

[1] Monireh Abdoos. 2020. A Cooperative Multiagent System for Traffic Signal Control Using Game Theory and Reinforcement Learning. IEEE Intelligent Transportation Systems Magazine 13, 4 (2020), 6–16.

[2] France Belanger, Janine S Hiller, and Wanda J Smith. 2002. Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. The Journal of Strategic Information Systems 11, 3 (2002), 245–270.

[3] Arnaud Berlioz, Arik Friedman, Mohamed Ali Kaafar, Roksana Boreli, and Shlomo Berkoskvy. 2015. Applying Differential Privacy to Matrix Factorization. In Proceedings of the 9th ACM Conference on Recommender Systems (Vienna, Austria). Association for Computing Machinery, New York, NY, USA, 107–114.

[4] Asia J. Biega, Peter Potash, Hal Daumé, Fernando Diaz, and Michèle Finck. 2020. Operationalizing the Legal Principle of Data Minimization for Personalization. Association for Computing Machinery, New York, NY, USA, 399–408.

[5] Lucas Bourdoule, Varun Chandrasekaran, Christopher A Choquette-Cho, Hengrui Jia, Adelin Travers, Baiwu Zhang, David Lie, and Nicolas Papernot. 2021. Machine unlearning. In 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 141–159.

[6] Yinzi Cao and Junfeng Yang. 2015. Towards making systems forget with machine unlearning. In 2015 IEEE Symposium on Security and Privacy. 463–480.

[7] 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.

[8] Chong Chen, Fei Sun, Min Zhang, and Bolin Ding. 2022. Recommendation Unlearning. arXiv:2201.06820 [cs.IR]

[9] Tsai-Wei Chen and S. Shyam Sundar. 2018. This App Would Like to Use Your Current Location to Better Serve You: Importance of User Assent and System Transparency in Personalized Mobile Services. Association for Computing Machinery, New York, NY, USA, 1–13.

[10] David N Chin. 2007. Information filtering, expertise and cognitive load. In International Conference on Foundations of Augmented Cognition. Springer, 75–83.

[11] Richard Chow, Hongxia Jin, Bart Knijnenburg, and Gokay Saldamli. 2013. Differential Data Analysis for Recommender Systems. In Proceedings of the 7th ACM Conference on Recommender Systems (Hong Kong, China). Association for Computing Machinery, New York, NY, USA, 323–326.

[12] Tianshu Chu, Jie Wang, Lara Codéca, and Zhaojian Li. 2019. Multi-agent deep reinforcement learning for large-scale traffic signal control. IEEE Transactions on Intelligent Transportation Systems 21, 3 (2019), 1086–1095.

[13] Paul Covington, Jay Adams, and Emre Sargin. 2016. Deep Neural Networks for YouTube Recommendations. In Proceedings of the 10th ACM Conference on Recommender Systems (Boston, Massachusetts, USA). Association for Computing Machinery, New York, NY, USA, 191–198.

[14] Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science 10, 1 (1999), 104–115.

[15] Josep Domingo-Ferrer, David Sánchez, and Alberto Blanco-Justicia. 2021. The Limits of Differential Privacy (and Its Misuse in Data Release and Machine Learning). Commun. ACM 64, 7 (jun 2021), 33–35.

[16] Cynthia Dwork and Aaron Roth. 2014. The Algorithmic Foundations of Differential Privacy. Found. Trends Theor. Comput. Sci. 9, 3–4 (aug 2014), 211–407.

[17] Joseph Farrell. 2012. Can privacy be just another good. J. on Telecomm. & High Tech. L. 10 (2012), 251.

[18] Chen Gao, Chao Huang, Dongsheng Lin, Depeng Jin, and Yong Li. 2020. DPLCF: Differentially Private Local Collaborative Filtering. Association for Computing Machinery, New York, NY, USA, 961–970.

[19] F. Maxwell Harper and Joseph A. Konstan. 2015. The MovieLens Datasets: History and Context. ACM Trans. Interact. Intell. Syst. 5, 4, Article 19 (dec 2015), 19 pages. https://doi.org/10.1145/2827872

[20] Xiangnan He, Kuan Deng, Xiang Wang, Yan Li, Yongdong Zhang, and Meng Wang. 2020. LightGCN: Simplifying and Powering Graph Convolution Network for Recommendation. Association for Computing Machinery, New York, NY, USA,
639–648.

[21] 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. 173–182.

[22] 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). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 173–182.

[23] Balázs Hidasi and Alexandros Karatzoglou. 2018. Recurrent neural networks with top-k gains for session-based recommendations. In Proceedings of the 27th ACM international conference on information and knowledge management (Torino, Italy). 843–852.

[24] Balázs Hidasi, Alexandros Karatzoglou, Linas Baltrunas, and Domonkos Tikk. 2016. Session-based Recommendations with Recurrent Neural Networks. In Proceedings of ICLR.

[25] 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. CoRR abs/1909.04847 (2019).

[26] Eugene Ie, Vihan Jain, Jing Wang, Sanmit Narvekar, Ritesh Agarwal, Rui Wu, Heng-Tze Cheng, Morgane Lustman, Vince Gatto, Paul Covington, et al. 2019. Reinforcement learning for slate-based recommender systems: A tractable decomposition and practical methodology. arXiv preprint arXiv:1905.12767 (2019).

[27] Dietmar Jannach, Lukas Lerche, Imran Kamekhkhosh, and Michael Jugov. 2015. What recommenders recommend: an analysis of recommendation biases and possible countermeasures. User Modeling and User-Adapted Interaction 25, 5 (2015), 427–491.

[28] Kaleervo Järvelin and Jaana Kekäläinen. 2002. Cumulated gain-based evaluation of IR techniques. ACM Transactions on Information Systems (TOIS) 20, 4 (2002), 422–446.

[29] Chunxiao Jiang, Linling Kuang, Zhu Han, Yong Ren, and Lajos Hanzo. 2017. Information credibility modeling in cooperative networks: Equilibrium and mechanism design. IEEE Journal on Selected Areas in Communications 35, 2 (2017), 432–448.

[30] Ginger Zhe Jin and Andrew Stivers. 2017. Protecting consumers in privacy and data Security: A perspective of information economics. Available at SSRN 3006172 (2017).

[31] Johan Källström and Fredrik Heintz. 2019. Tunable dynamics in agent-based simulation using multi-objective reinforcement learning. In Adaptive and Learning Agents Workshop (ALA-19) at AAMAS, Montreal, Canada, May 13-14, 2019. 1–7.

[32] Wang-Cheng Kang and Julian McAuley. 2018. Self-attentive sequential recommendation. In 2018 IEEE International Conference on Data Mining (ICDM). IEEE, 197–206.

[33] Michael N Katehakis and Arthur F Veinott Jr. 1987. The multi-armed bandit problem: decomposition and computation. Mathematics of Operations Research 12, 2 (1987), 262–268.

[34] Diederik P Kingma and Jimmy Ba. 2015. Adam: A Method for Stochastic Optimization. In ICLR (Poster).

[35] Bart P. Knijnenburg and Alfred Kobsa. 2013. Making Decisions about Privacy: Information Disclosure in Context-Aware Recommenders. In Proceedings of the Sixth Conference on Recommender Systems (Dublin, Ireland). Association for Computing Machinery, New York, NY, USA, 43–50.

[36] Bart P. Knijnenburg and Alfred Kobsa. 2013. Making Decisions about Privacy: Information Disclosure in Context-Aware Recommender Systems. ACM Trans. Interact. In tell. Syst. 3, 3, Article 20 (oct 2013), 23 pages.

[37] Yehuda Koren, Robert Bell, and Chris Volinsky. 2009. Matrix Factorization Techniques for Recommender Systems. ACM Trans. Interact. In tell. Syst. 3, 3, Article 20 (oct 2013), 23 pages.

[38] Karl Krauth, Sarah Dean, Alex Zhao, Wenshuo Guo, Mihaela Curmei, Benjamin Recht, and Michael I Jordan. 2020. Do Offline Metrics Predict Online Performance in Recommender Systems? arXiv preprint arXiv:2011.07931 (2020).

[39] Walid Krichene and Steffen Rendle. 2020. On Sampled Metrics for Item Recommendation. In Proceedings of the 26th International Conference on World Wide Web. 173–182.

[40] Robert S. Laufer and Maxine Wolfe. 1977. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues 33, 3 (1977), 22–42.

[41] Chao Li, Zhiyuan Liu, Mengmeng Wu, Yuchi Xu, Huan Zhao, Peipei Huang, Guoliang Kang, Qiwei Chen, Wei Li, and Dik Lun Lee. 2019. Multi-Interest Network with Dynamic Routing for Recommendation at Tmall. In Proceedings of the 28th ACM International Conference on Information and Knowledge Management (Beijing, China). Association for Computing Machinery, New York, NY, USA, 1748–1757.

[42] Wenhui Lin. 2019. Valuing intrinsic and instrumental preferences for privacy. Available at SSRN 3406412 (2019).

[43] Tesary Lin. 2019. Valuing intrinsic and instrumental preferences for privacy. Available at SSRN 3406412 (2019).
[44] Yujie Lin, Pengjie Ren, Zhumin Chen, Zhaochun Ren, Dongxiao Yu, Jun Ma, Maarten de Rijke, and Xiuzhen Cheng. 2020. Meta Matrix Factorization for Federated Rating Predictions. In Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval. Association for Computing Machinery, New York, NY, USA, 981–990.

[45] Greg Linden, Brent Smith, and Jeremy York. 2003. Amazon.Com Recommendations: Item-to-Item Collaborative Filtering. IEEE Internet Computing 7, 1 (jan 2003), 76–80.

[46] Eli Lucherini, Matthew Sun, Amy Winecoff, and Arvind Narayanan. 2021. T-RECS: A simulation tool to study the societal impact of recommender systems. arXiv preprint arXiv:2107.08959 (2021).

[47] Fuyu Lv, Taiwei Jin, Changlong Yu, Fei Sun, Quan Lin, Keping Yang, and Wilfred Ng. 2019. SDM: Sequential deep matching model for online large-scale recommender system. In Proceedings of the 28th ACM International Conference on Information and Knowledge Management. 2635–2643.

[48] Jonathan R. Mayer and John C. Mitchell. 2012. Third-Party Web Tracking: Policy and Technology. In 2012 IEEE Symposium on Security and Privacy. 413–427.

[49] Frank McSherry and Ilya Mironov. 2009. Differentially Private Recommender Systems: Building Privacy into the Netflix Prize Contenders. In Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (Paris, France). Association for Computing Machinery, New York, NY, USA, 627–636.

[50] Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov. 2019. Exploiting unintended feature leakage in collaborative filtering. In 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 691–706.

[51] Lorenzo Minto, Moritz Haller, Benjamin Livshits, and Hamed Haddadi. 2021. Stronger Privacy for Federated Collaborative Filtering With Implicit Feedback. In Fifteenth ACM Conference on Recommender Systems. Association for Computing Machinery, New York, USA, 342–350.

[52] Andriy Mnih and Russ R Salakhutdinov. 2008. Probabilistic Matrix Factorization. In Advances in Neural Information Processing Systems, Vol. 20. Curran Associates, Inc., 1257–1264.

[53] Khalil Muhammad, Qinqin Wang, Diarmuid O’Reilly-Morgan, Elias Tragos, Barry Smyth, Neil Hurley, James Geraci, and Aonghus Lawlor. 2020. FedFast: Going Beyond Average for Faster Training of Federated Recommender Systems. In Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (Virtual Event, CA, USA). Association for Computing Machinery, New York, NY, USA, 1234–1242.

[54] Milad Naser, Reza Shokri, and Amir Houmansadr. 2019. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. In 2019 IEEE symposium on security and privacy (SP). IEEE, 739–753.

[55] Blażej Osinski, Adam Jakubowski, Pawel Ziczena, Piotr Milos, Christopher Galias, Silviu Homoceanu, and Henryk Michalewski. 2020. Simulation-based reinforcement learning for real-world autonomous driving. In 2020 IEEE International Conference on Robotics and Automation (ICRA). IEEE, 6411–6418.

[56] Tao Qi, Fangzhao Wu, Chuhuan Wu, Yongfeng Huang, and Xing Xie. 2020. Privacy-Preserving News Recommendation Model Learning. In Findings of the Association for Computational Linguistics: EMNLP 2020. Association for Computational Linguistics, Online, 1423–1432.

[57] Massimo Quadranra, Paolo Cremonesi, and Dietmar Jannach. 2018. Sequence-Aware Recommender Systems. ACM Comput. Surv. 51, 4, Article 66 (jul 2018), 36 pages.

[58] Kanishka Rao, Chris Harris, Alex Irpan, Sergey Levine, Julian Ibarz, and Mohi Khansari. 2020. Rl-cyclegan: Reinforcement learning aware simulation-to-real. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 11157–11166.

[59] Steffen Rendle, Christoph Freudenthaler, and Lars Schmidt-Thieme. 2010. Factorizing Personalized Markov Chains for Next-Basket Recommendation. In Proceedings of the 19th International Conference on World Wide Web (Raleigh, North Carolina, USA). Association for Computing Machinery, New York, NY, USA, 811–820.

[60] Pedram Samadi, Hamed Mohsenian-Rad, Robert Schober, and Vincent WS Wong. 2012. Advanced demand side management for the future smart grid using mechanism design. IEEE Transactions on Smart Grid 3, 3 (2012), 1170–1180.

[61] Badrul Sarwar, George Karypis, Joseph Konstan, and John Riedl. 2001. Item-Based Collaborative Filtering Recommendation Algorithms. In Proceedings of the 10th International Conference on World Wide Web (Hong Kong, Hong Kong). Association for Computing Machinery, New York, NY, USA, 285–295.

[62] Guy Shani, David Heckerman, and Ronen I. Brafman. 2005. An MDP-Based Recommender System. Journal of Machine Learning Research 6, 43 (2005), 1265–1295. http://jmlr.org/papers/v6/shani05a.html

[63] Jing-Cheng Shi, Yang Yu, Qing Da, Shi-Yong Chen, and An-Xiang Zeng. 2019. Virtual-Taobao: Virtualizing Real-World Online Retail Environment for Reinforcement Learning. In Proceedings of the AAAI Conference on Artificial Intelligence. 4902–4909.

[64] Hyejin Shin, Sungwook Kim, Junbum Shin, and Xiaokui Xiao. 2018. Privacy enhanced matrix factorization for recommendation with local differential privacy. IEEE Transactions on Knowledge and Data Engineering 30, 9 (2018),
[65] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals’ Concerns about Organizational Practices. *MIS Quarterly* 20, 2 (1996), 167–196.

[66] Fei Sun, Jun Liu, Jian Wu, Changhua Pei, Xiao Lin, Wenwu Ou, and Peng Jiang. 2019. BERT4Rec: Sequential Recommendation with Bidirectional Encoder Representations from Transformer. In *Proceedings of the 28th ACM International Conference on Information and Knowledge Management* (Beijing, China). Association for Computing Machinery, New York, NY, USA, 1441–1450.

[67] Richard S. Sutton and Andrew G. Barto. 2018. *Reinforcement learning: An introduction*. MIT press.

[68] Huan Tang. 2019. The value of privacy: Evidence from online borrowers. *Working Paper, HEC Paris* (2019).

[69] Josh Tobin, Rachel Fong, Alex Ray, Jonas Schneider, Wojciech Zaremba, and Pieter Abbeel. 2017. Domain randomization for transferring deep neural networks from simulation to the real world. In *2017 IEEE/RSJ international conference on intelligent robots and systems (IROS)*. IEEE, 23–30.

[70] Hao Wang, Naiyan Wang, and Dit-Yan Yeung. 2015. Collaborative Deep Learning for Recommender Systems. In *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (Sydney, NSW, Australia). Association for Computing Machinery, New York, NY, USA, 1235–1244.

[71] Qinyong Wang, Hongzhi Yin, Tong Chen, Junliang Yu, Alexander Zhou, and Xiangliang Zhang. 2021. Fast-adapting and Privacy-preserving Federated Recommender System. *The VLDB Journal* (2021).

[72] Suhang Wang, Yilin Wang, Jiliang Tang, Kai Shu, Suhas Ranganath, and Huan Liu. 2017. What Your Images Reveal: Exploiting Visual Contents for Point-of-Interest Recommendation. In *Proceedings of the 26th International Conference on World Wide Web* (Perth, Australia). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 391–400.

[73] Hongyi Wen, Longqi Yang, Michael Sobolev, and Deborah Estrin. 2018. Exploring Recommendations under User-Controlled Data Filtering. *Association for Computing Machinery, New York, NY, USA, 72–76.*

[74] Xu Xie, Fei Sun, Xiaoyong Yang, Zhao Yang, Jinyang Gao, Wenwu Ou, and Bin Cui. 2021. Explore User Neighborhood for Real-time E-commerce Recommendation. In *2021 IEEE 37th International Conference on Data Engineering (ICDE)*. IEEE, 2464–2475.

[75] Yu Xin and Tommi Jaakkola. 2014. Controlling privacy in recommender systems. In *Advances in Neural Information Processing Systems*, Vol. 27. Curran Associates, Inc., 2618–2626.

[76] 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).

[77] Sirui Yao and Bert Huang. 2017. Beyond parity: Fairness objectives for collaborative filtering. *arXiv preprint arXiv:1705.08804* (2017).

[78] Rex Ying, Ruining He, Kaifeng Chen, Pong Eksombatchai, William L. Hamilton, and Jure Leskovec. 2018. Graph Convolutional Neural Networks for Web-Scale Recommender Systems. In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (London, United Kingdom). Association for Computing Machinery, New York, NY, USA, 974–983.

[79] Bo Zhang and S. Shyam Sundar. 2019. Proactive vs. reactive personalization: Can customization of privacy enhance user experience? *International Journal of Human-Computer Studies* 128 (2019), 86–99.

[80] Bo Zhang, Na Wang, and Hongxia Jin. 2014. Privacy Concerns in Online Recommender Systems: Influences of Control and User Data Input. In *10th Symposium On Usable Privacy and Security*. 159–173.

[81] Minxing Zhang, Zhaochun Ren, Zihan Wang, Pengjie Ren, Zhunmin Chen, Pengfei Hu, and Yang Zhang. 2021. Membership Inference Attacks Against Recommender Systems. , 16 pages.

[82] Ligeng Zhu, Zhijian Liu, and Song Han. 2019. Deep Leakage from Gradients. In *Advances in Neural Information Processing Systems*, Vol. 32. Curran Associates, Inc.