

A Privacy-Aware Framework for Targeted Advertising

Wei Wang^a, Linlin Yang^b, Yanjiao Chen^a, Qian Zhang^{a,*}

^a*Department of Computer Science and Engineering*

^b*Fok Ying Tung Graduate School*

Hong Kong University of Science and Technology, Hong Kong

Abstract

Much of today's Internet ecosystem relies on online advertising for financial support. Since the effectiveness of advertising heavily depends on the relevance of the advertisements (ads) to user's interests, many online advertisers turn to targeted advertising through an ad broker, who is responsible for personalized ad delivery that caters to user's preference and interest. Most of existing targeted advertising systems need to access the users' profiles to learn their traits, which, however, has raised severe privacy concerns and make users unwilling to involve in the advertising systems. Spurred by the growing privacy concerns, this paper proposes a privacy-aware framework to promote targeted advertising. In our framework, the ad broker sits between advertisers and users for targeted advertising and provides certain amount of compensation to incentivize users to click ads that are interesting yet sensitive to them. The users determine their clicking behaviors based on their interests and potential privacy leakage, and the advertisers pay the ad broker for ad clicking. Under this framework, the optimal strategies of the advertisers, the ad broker and the users are analyzed by formulating the problem as a three-stage game, in which a unique Nash Equilibrium is achieved. In particular, we analyze the players' behaviors for the scenarios of independent advertisers and competing advertisers. Extensive simulations have been conducted and the results validate the effectiveness of the proposed framework by showing that the utilities of all entities are significantly

*Corresponding author. Tel.: +852 23588766
Email address: qianzh@cse.ust.hk (Qian Zhang)

improved compared with traditional systems.

Keywords: Targeted Advertising, Privacy, Game Theory

1. Introduction

Online advertising provides financial support for a large portion of today's Internet ecosystem, and is displayed in a variety of forms embedded in web sites, emails, videos and so on. As the effectiveness of advertising largely depends on the relevance between the delivered advertisements (ads) and users' interests, a popular paradigm for current online advertising system is targeted advertising, where advertisers hire an ad broker to deliver ads to potentially interested users by analyzing users' online profiles or behaviors [1, 2]. Targeted advertising is beneficial to both advertisers and users: advertisers can gain higher revenue by advertising to users with a strong potential to purchase, and the users in turn receive more pertinent and useful ads that match their preferences and interests. A recent survey [3] revealed that targeted advertising brings 2.68 times revenue per ad compared with non-targeted advertising. Due to the increased effectiveness and benefits, a number of advertisers around the world have already turned to online targeted advertising systems. Examples of such advertising systems include Google AdWords [4] that deliver customized ads based on search items, and Ink TAD [5] that pushes ads according to location information revealed in user's emails.

Although targeted advertising benefits both advertisers and users, it has raised severe privacy concerns. A recent survey [6] of 2,253 participates conducted in 2012 reported that the majority of respondents expressed disapproval of targeted advertising due to privacy disclosure. Such privacy threats come from the fact that ad brokers aggressively track users' online behaviors to obtain their preferences and interests, which can be sensitive to the users. For example, the behavior of searching for a certain kind of medicine implies that the user is likely to have certain relevant disease, whose disclosure is considered as a violation of the user's privacy. Moreover, ad brokers rarely have clear state-

ments about how the obtained behavioral data will be used and whom the data will be shared with. Untrusted ad brokers may sell such personal information to some adversaries without the user’s permission. Being aware of such privacy risks, users are reluctant to embrace the practice of targeted advertising [7], which hinders the effectiveness of online advertising systems.

To maintain the merits brought by targeted advertising, it is essential to incentivize users to participate in such systems. Existing studies [8, 9, 10] have focused on privacy preserving mechanisms to encourage users to involve in the targeted advertising systems. These mechanisms either assume another trusted entity sitting between users and ad brokers [8, 9], or require users to send perturbed clicking information to hide users’ true data. However, these changes made on the framework of existing targeted advertising systems provide privacy protection at the cost of the benefits of ad brokers or advertisers. The ad brokers may not be in favor of introducing an extra entity to share their ad targeting duty, which is the main source of their revenue. Similarly, the advertisers may be dissatisfied with the perturbed clicking information as perturbation undermines the accuracy of click information, which normally determines their payments [11]. Without guaranteed revenue, the advertisers and ad brokers naturally tend to maintain the adoption of traditional targeted advertising systems instead of upgrading the systems to provide privacy protection. This conflict between users and advertisers/ad brokers hinders the adoption of privacy-aware mechanisms in advertising. To promote the adoption of the privacy-aware advertising systems, the interests of all entities should be guaranteed, which, unfortunately has not yet been addressed by existing proposals.

In this paper, we propose a privacy-aware framework to boost the adoption of privacy preserving targeted advertising systems. Users, the ad broker and advertisers are assumed to be rational and selfish entities, who care only about their own interests. To ensure the interests of all entities, our framework introduces an economic compensation mechanism for privacy leakage. Such economic compensation for privacy loss has already been widely considered in the literature [12, 13, 14]. Besides, many companies, including Bynamite, Yahoo,

and Google, are also engaging in the purchase of users' private information in exchange for monetary or non-monetary compensation [15, 13]. Under the proposed framework, the ad brokers compensate economically for the users' privacy leakage in order to incentivize users to click their interested ads. On the one hand, the users, with the expectation of receiving compensation, are inclined to click ads of interests. On the other hand, as the compensation can improve click-through rate and bring the ad broker more revenue, the ad broker is willing to provide certain amount of compensation for users whose ad clicks reveal their private interests. However, to support this framework, there are still several questions that need to be answered. First and foremost, in order to compensate privacy loss, it is essential to quantify privacy information leakage in ad clicks. Second, how much compensation should be provided for each user? The more compensation provided, the more inclined users are to click ads; while the ad broker pays more for the users' privacy loss. Moreover, how should advertisers pay the ad broker for the ad clicks they benefit from? The amount of payment to the ad broker has an impact on the privacy loss compensation allocated to users, which in turn affects the click-through rates and advertisers' revenue. In this paper, we answer all these questions via game theory analysis. In particular, we propose an ad dissemination protocol to protect the users' privacy to a large extent, and formulate the interactions among all entities as a three-stage game, where each entity aims to maximize its own utility.

The main contributions of this paper are summarized as follows.

- We propose a privacy-aware framework for targeted advertising to motivate users, the ad broker, and advertisers to be engaged in the targeted advertising systems. This framework requires no modifications on existing targeted advertising systems, and takes the incentives of all parties into consideration. In our framework, the ad broker provides a certain amount of compensation for the users' privacy leakage from ad clicks in order to encourage users to click their interested ads, which in turn improves the click-through rate and brings in more revenue for the ad broker and

advertisers.

- 90 • We model the framework as a three-stage Stackelberg game, in which all entities are considered to be selfish, targeting at maximizing their own utilities by selecting optimal strategies. We analyze the cooperation and competition relationship among users, the ad broker, and advertisers, and derive the Nash Equilibrium.
- 95 • We further analyze the competition among advertisers who share the whole market. We model the market sharing scenario as a non-cooperative game and prove the existence of the Nash Equilibrium.
- We conduct numerical simulations to evaluate the proposed framework. The results verify that the utilities of all entities are notably enhanced,
100 which provides strong motivation for the ad broker and advertisers to implement the compensation policy and users to embrace the targeted advertising.

The rest of the paper is organized as follows. Section 2 describes the system model. Section 3 introduces the compensation framework. In Section 4, we
105 model the framework as a three-stage game and analyze the optimal strategies of advertisers, the ad broker and users. We further discuss the competition among advertisers for market sharing. Numerical results are shown in Section 5 and related works are reviewed in Section 6, followed by the conclusion in Section 7.

110 2. System Model

In this section, we describe the system model, including the targeted advertising system and privacy sensitivity.

2.1. Targeted Advertising System

We adopt the most popular advertiser-broker-user advertising architecture
115 on today's Internet. Figure 1 illustrates such a targeted advertising system

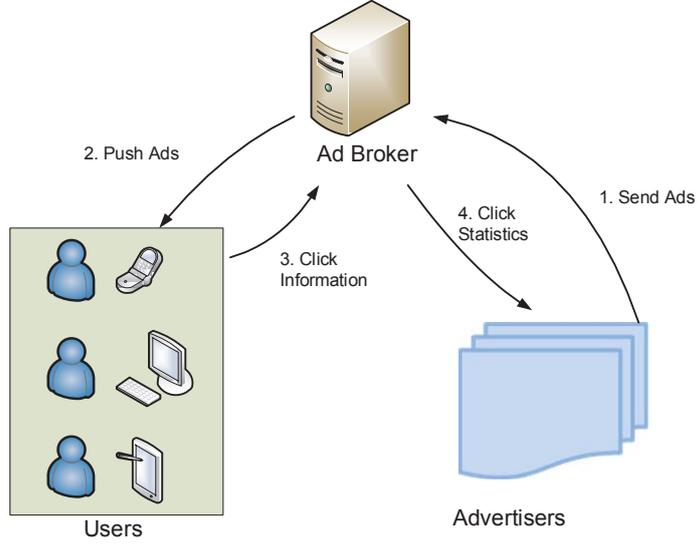


Figure 1: Structure of privacy-aware targeted advertising system

which comprises of a set of advertisers, one ad broker and a group of users. Advertisers are interested in displaying ads to the users of potential interests, and are willing to pay a certain amount money for the ads that are viewed by the interested users. Ads are delivered by an advertising platform (e.g.,
 120 Google’s AdWords) run by the ad broker. The advertising platform collects ads from advertisers and disseminate ads to the targeted users according to the ad broker’s scheduling algorithm.

Ad dissemination is scheduled over a series of time slots. In each time slot, there are a set of active users, that is, the users who are viewing a device that
 125 can display an ad in that time slot. A set of ads from different advertisers are selected based on the preferences of the active users in that time slot. We assume that the ad broker selects at most one ad from an advertiser in each time slot. In order to keep notation simple, we consider the ad dissemination in one time slot. We denote the set of active users and the set of ads in a time
 130 slot as $\{S_i : i = 1, \dots, N\}$ and $\{A_j : j = 1, \dots, K\}$, respectively.

To preserve users' privacy, we assume that the user profiles are kept on their local devices and cannot be accessed by the ad broker or advertisers [10]. In line with the privacy preserving online advertising systems [9, 10, 16], we focus on privacy leakage via ad click, while we do not consider the privacy leakage via web browsing tracking as it occurs outside the advertising system. To predict the users' preferences, the ad broker collects the ad click information, which, however, may compromise users' privacy. In the following section, we quantify privacy leakage from ad clicks. We also assume that there is no click fraud, as click fraud can be addressed by existing solutions [17, 18].

2.2. Privacy Sensitivity

On the one hand, the privacy level of ad click behavior is considered to be content-dependent: clicking different kinds of ads leads to different levels of privacy leakage. For example, clicking a medical ad may imply that you have a certain kind of disease, which is normally very sensitive to the users; whereas, clicking an umbrella ad usually leaks little privacy of the users. To quantify the content-dependent privacy level, we introduce a privacy factor α_j to present the sensitivity of an ad A_j . The content of an ad with larger α_j is more sensitive. For example, the privacy factor α_{j_1} of a medical ad A_{j_m} is normally larger than the privacy factor α_{j_2} of an umbrella ad A_{j_u} .

On the other hand, the privacy level of ad click behavior is also related to the total number of users who have clicked it. According to the notion of k -anonymity [19], when a user's information is identical with more users (k is larger), it is harder for adversaries to identify the user by looking at the clicking behavior, meaning that less information is leaked. Thus, we define the privacy leakage of clicking an ad A_j as α_j/n_j , where n_j is the total number of users clicking A_j .

3. The Compensation Framework

In this section, we propose a privacy-aware compensation framework to promote targeted advertising with the consideration of privacy leakage. The target

160 of the framework is to establish a win-win situation among all entities in the targeted advertising system. In the framework, with the promise of privacy leakage compensation, the sensitive users are incentivized to view their interested ads. The ad broker and advertisers earn more revenue from more ad clicks. It is noteworthy that our proposed framework is built on top of the existing
 165 advertiser-broker-user advertising architecture as described in Section 2, and introduces no new parties.

The ad broker assists advertisers to target interested users and deliver ads to those users. Advertisers yield higher revenue by delivering ads to desired users via the ad broker [1]. In return, the ad broker charges the advertisers for each
 170 ad click. This business model is prevalent in the current Internet ecosystem. Recall that users are reluctant to click their interested ads when the ad contents are sensitive and their private preferences can be revealed to the ad broker. To motivate users to click their interested ads, the proposed framework introduces a compensation mechanism in which the ad broker puts forward a total sum
 175 of M_j compensation amount, which is distributed to users who have clicked sensitive ads.

Under the compensation framework, all entities are considered to be rational and aim to maximize their own utilities. Advertisers gain revenue from clicks. Since in each time slot, each ad corresponds to one advertiser. For simplicity, we use A_j to denote the advertiser who distributes ad A_j . For every click on A_j , the corresponding advertiser gains an average revenue of Q_j . The expense of advertisers is the money they pay to the ad broker. We denote the amount of payment for each click on A_j as P_j . The utility of advertiser A_j is defined as its revenue from clicks minus the fee it pays to the the ad broker, which is expressed as

$$U_j^a = n_j Q_j - n_j P_j, \quad (1)$$

where n_j is the total number of clicks on ad A_j .

The ad broker receives money from advertisers and decides the total amount of compensation M_j to be paid to all users for clicking ad A_j . The compensation

M_j is then allocated evenly to each user who has clicked ad A_j . The utility of the ad broker is defined as the total revenue from all advertisers minus the total money paid to users.

$$U^b = \sum_j n_j P_j - \sum_j M_j. \quad (2)$$

Users decide whether to click their interested ads that are delivered to their devices based on the amount of compensation and their privacy loss. Let $R_{i,j} = 0$ denote that user S_i decides not to click ad A_j and $R_{i,j} = 1$ denote that user S_i decides to click ad A_j . Then, the total number of clicks for ad A_j is $n_j = \sum_q R_{q,j}$. The overall compensation that user S_i receives is

$$C_i = \sum_j M_j \frac{R_{i,j}}{\sum_q R_{q,j}}. \quad (3)$$

Studies have shown that different users have different levels of privacy sensitivity [20, 21]. Accordingly, let $\{\omega_i : i = 1, \dots, N\}$ represent privacy sensitivities of different users.

As described earlier, ad clicks leak users' preferences to the ad broker. The privacy leakage of clicking ad A_j is $\alpha_j/n_j = \alpha_j/\sum_q R_{q,j}$. Therefore, the total amount of user's privacy leakage is

$$L_i = \frac{\alpha_j R_{i,j}}{\sum_q R_{q,j}}. \quad (4)$$

Then, the utility of user S_i is defined as the amount of money it receives from the ad broker minus the amount of money needed to compensate the user for privacy leakage

$$\begin{aligned} U_i^s &= C_i - \omega_i L_i \\ &= \sum_j M_j \frac{R_{i,j}}{\sum_q R_{q,j}} - \omega_i \sum_j \frac{\alpha_j R_{i,j}}{\sum_q R_{q,j}}, \end{aligned} \quad (5)$$

where ω_i is defined as the equivalent amount of compensation desired by user S_i for every unit of privacy loss.

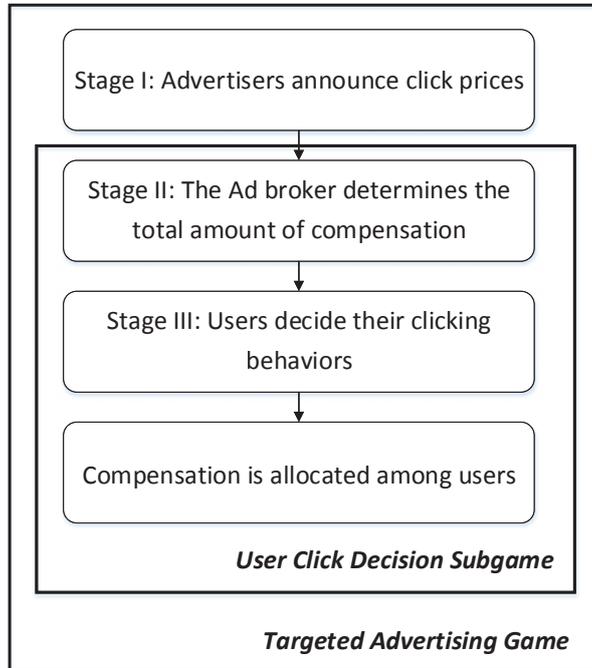


Figure 2: The procedure of targeted advertising and ad clicking.

4. Game Theory Analysis

In this section, we cast the targeted advertising under the compensation
185 framework as a three-stage Stackelberg game, and analyze the best strategies
of all entities based on their utilities. We consider two advertising scenarios:
independent advertisers who are engaged in independent markets and market
sharing advertisers who compete against each other.

The targeted advertising game consists of three stages, as illustrated in Fig-
190 ure 2. In the first stage of the game, advertisers announce the price of each ad
click they will pay to the ad broker. In the second stage, observing the price it
receives for every click, the ad broker determines the amount of money it com-
pensates all users. In the last stage, users decide whether or not to click the ads.

All players act in a non-cooperative way as they make decisions independently.

195 The whole game can be viewed as the combination of a user click decision subgame and a targeted advertising subgame. In the user click decision subgame, the ad broker acts as the leader because it determines the total amount of compensation, and leads the ad delivery procedure. The ad broker first announces the total amount of compensation and pushes ads to intended users
 200 according to its scheduling algorithm. The users play as followers, and decide their clicking behavior based on their evaluation of privacy loss and expected compensation. In the targeted advertising subgame, the advertisers play as leaders, as they initiate the whole advertising procedure and pay the ad broker to distribute their ads. The ad broker acts as the follower to initiate the user
 205 click decision subgame.

4.1. Targeted Advertising for Independent Advertisers

We first analyze the targeted advertising game for independent advertisers, and use backward induction to derive Nash Equilibrium, where the optimal strategies for advertisers, the ad broker and users are obtained accordingly.

210 4.1.1. User Clicking Behavior Analysis

We first analyze users' decision making process. Note that user S_i 's utility not only depends on its own decisions, but also on other users' choices. Let $\{R_{i,j} : j = 1, \dots, K\}$ denote user S_i 's strategy and $\{R_{-i,j} : j = 1, \dots, K\}$ denote the strategies of all the other users. The utility of user S_i is $U_i^s(R_{i,j}, R_{-i,j})$. Then, the best response of S_i is given by

$$R_{i,j}^* = \arg \max_{R_{i,j}} U_i^s(R_{i,j}, R_{-i,j}). \quad (6)$$

Given the strategies of other users, the best response of S_i is its optimal strategy. S_i will not deviate from its best response unilaterally as it can gain nothing. If every user adopts the best response, Nash Equilibrium is reached.

If every user employs the best response with regard to other users' decisions,
 215 no users have motivation to deviate from its best response unilaterally. As such, Nash Equilibrium is reached.

Theorem 1. *When the following condition*

$$M_j/\alpha_j \geq \min_i\{\omega_i\} \quad (7)$$

is satisfied, there exists a Nash Equilibrium for the game among users and the optimal strategy of S_i is

$$R_{i,j}^* = \begin{cases} 1, & \omega_i \leq M_j/\alpha_j \\ 0, & \omega_i > M_j/\alpha_j \end{cases} \quad (8)$$

Proof. From Equation (5), we have

$$U_i^s = \sum_j (M_j - \omega_i \alpha_j) \frac{R_{i,j}}{\sum_q R_{q,j}}. \quad (9)$$

When $M_j \geq \omega_i \alpha_j$, selecting $R_{i,j} = 1$ can increase S_i 's utility. Whereas, if $M_j < \omega_i \alpha_j$, selecting $R_{i,j} = 0$ can avoid decreasing S_i 's utility. So U_i^s can be maximized when S_i determines the value of $R_{i,j}$ according to Equation (8), which is S_i 's optimal strategy. Note that Equation (7) guarantees that the denominator of Equation (9) is non-zero. Every user can obtain its optimal strategy by this mechanism. Thus, Nash Equilibrium is reached when they all
 225 adopt the optimal strategy. \square

4.1.2. Optimal Compensation Strategy of Ad Broker

When the ad broker decides its strategy $\{M_j : j = 1, \dots, K\}$, users will make their decisions according to Theorem 1. Accordingly, the ad broker can determine the optimal strategy. As the leader of the user click decision subgame, the
 230 ad broker is aware of the impact of the total compensation amount on users' decisions. Taking into account users' possible responses, the ad broker can obtain its optimal strategy to maximize its profit.

Proposition 1. *The ad broker has a unique optimal strategy that can maximize its utility.*

Proof. Based on Equation (2), we have

$$U^b = \sum_j (P_j n_j - M_j), \quad (10)$$

where $n_j = \sum_i R_{i,j} = \left| \left\{ \omega_i \leq \frac{M_j}{\alpha_j} : i = 1, 2, \dots, N \right\} \right|$. Assume $\{\omega_1, \omega_2, \dots, \omega_N\}$ follow a certain kind of distribution, whose probability distribution function is $f(\omega)$. As N is a very large number (there are many end users in the system), n_j can be calculated in this way

$$n_j = N \int_0^{\frac{M_j}{\alpha_j}} f(\omega) d\omega. \quad (11)$$

So we have

$$U^b = \sum_j \left(P_j N \int_0^{\frac{M_j}{\alpha_j}} f(\omega) d\omega - M_j \right), \quad (12)$$

$$\frac{dU^b}{dM_j} = \sum_j \left(\frac{P_j N}{\alpha_j} f\left(\frac{M_j}{\alpha_j}\right) - 1 \right), \quad (13)$$

$$\frac{d^2U^b}{dM_j^2} = \sum_j \left(\frac{P_j N}{\alpha_j^2} f'\left(\frac{M_j}{\alpha_j}\right) \right). \quad (14)$$

As N is very large, there exists two points where $f(\omega) = \frac{\alpha_j}{P_j N}$. Only the right one has a negative derivative, so there exists a unique set of $\{M_j : j = 1, \dots, K\}$, that makes $\frac{dU^b}{dM_j} = 0$ and $\frac{d^2U^b}{dM_j^2} < 0$. To sum up, the ad broker can maximize its utility by the following unique strategy

$$M_j^* = \alpha_j f^{-1}\left(\frac{\alpha_j}{P_j N}\right), \quad (15)$$

235 where we select the larger value of $f^{-1}\left(\frac{\alpha_j}{P_j N}\right)$. □

To obtain a closed-form of the ad broker's optimal strategy M_j^* , we assume that users' privacy sensitivities follow Gaussian distribution $N(\mu, \sigma^2)$, which is commonly used to model real-value random variables. In accordance with the three-sigma rule, the probability that a variable lies within $[\mu - 3\sigma, \mu + 3\sigma]$ is 99.74%, and thus the values outside this interval can be neglected. Hence, we can use Gaussian distribution $N(\mu, \sigma^2)$ to model users' privacy sensitivities with

the constraint $\mu > 3\sigma$. In this circumstance, the ad broker's optimal strategy is expressed as

$$M_j^* = \alpha_j \left(\mu + \sqrt{2\sigma^2 \ln \frac{P_j N}{\alpha_j \sqrt{2\pi\sigma^2}}} \right). \quad (16)$$

4.1.3. Optimal Ad Pricing Strategy of Advertiser

In the targeted advertising subgame, advertisers determine their optimal strategies based on the ad broker's compensation strategy.

Proposition 2. *There exists optimal strategies for advertisers, and when users' privacy sensitivities follow Gaussian distribution, the optimal strategy for every advertiser is unique.*

Proof. From Equation (1) and (11), we have

$$U_j^a = (Q_j - P_j)N \int_0^{\frac{M_j^*}{\alpha_j}} f(\omega) d\omega. \quad (17)$$

It can be seen that $U_j^a(P_j)$ is a continuous function and its upper bound is Q_j . So there exists P_j^* , which is the optimal strategy that maximizes U_j^a .

We further analyze the circumstance where $\{\omega_i : i = 1, \dots, N\}$ follow the Gaussian distribution $N(\mu, \sigma^2)$. To simplify analysis, it is equal to consider function $\ln U_j^a$. We have

$$\frac{d(\ln U_j^a)}{dP_j} = -\frac{1}{Q_j - P_j} + \frac{f\left(\frac{M_j^*}{\alpha_j}\right)}{\int_0^{\frac{M_j^*}{\alpha_j}} f(\omega) d\omega} \frac{d\left(\frac{M_j^*}{\alpha_j}\right)}{dP_j}, \quad (18)$$

where $P_j \in (0, Q_j)$. Together with Equation (16), we obtain

$$\frac{d(\ln U_j^a)}{dP_j} = -\frac{1}{Q_j - P_j} + \frac{\alpha_j \sigma^2}{N P_j^2 \sqrt{2\sigma^2 \ln \frac{N P_j}{\alpha_j \sqrt{2\pi\sigma^2}}} \int_0^{\frac{M_j^*}{\alpha_j}} f(\omega) d\omega}. \quad (19)$$

It is obvious that $\frac{d(\ln U_j^a)}{dP_j}$ is a decreasing function with regard to P_j , that is $\frac{d^2(\ln U_j^a)}{dP_j^2} < 0$, and the following two equations

$$\lim_{P_j \rightarrow 0^+} \frac{d(\ln U_j^a)}{dP_j} = +\infty, \quad (20)$$

$$\lim_{P_j \rightarrow Q_j^-} \frac{d(\ln U_j^a)}{dP_j} = -\infty \quad (21)$$

hold. So there is one unique P_j^* , where $\frac{d(\ln U_j^a)}{dP_j} = 0$, and this P_j^* is the unique
 245 optimal strategy for advertiser A_j . \square

4.2. Targeted Advertising for Market Sharing Advertisers

In the model analyzed above, we assume that for every click advertiser A_j gains a constant revenue of Q_j , which only stands for independent advertisers. For competing advertisers who send ads about similar products or services, the whole market size is limited and shared by those advertisers. Therefore, in this subsection, we discuss a more realistic model, for which we assume the whole market size is Q . The market size for advertiser A_j is positively related to the proportion of clicks on its ad to the total clicks on all similar ads, that is $\frac{n_j}{\sum_q n_q}$. So the utility of A_j is

$$U_j^a = Q \frac{n_j}{\sum_q n_q} - P_j n_j. \quad (22)$$

As advertisers are aware of the ad broker's reaction to their strategies, they can decide their optimal strategies accordingly.

Proposition 3. *There exists a unique optimal strategy for an advertiser when
 250 users' privacy sensitivities follow Gaussian distribution and other advertisers' strategies are fixed.*

Proof. When $\{\omega_i : i = 1, \dots, N\}$ follow the Gaussian distribution $N(\mu, \sigma^2)$, we have

$$\frac{d(U_j^a)}{dP_j} = \left(Q \frac{\sum_{q \neq j} n_q}{(\sum_q n_q)^2} - P_j \right) \frac{N \sigma f\left(\frac{M_j}{\alpha_j}\right)}{P_j \sqrt{2 \ln \frac{P_j N}{\alpha_j \sqrt{2\pi\sigma^2}}}} - n_j \quad (23)$$

It can be easily seen that $\frac{d(U_j^a)}{dP_j}$ is a decreasing function with regard to P_j , that is $\frac{d^2(U_j^a)}{dP_j^2} < 0$, and the following two Equations

$$\lim_{P_j \rightarrow 0^+} \frac{d(U_j^a)}{dP_j} = +\infty, \quad (24)$$

$$\lim_{P_j \rightarrow -\infty} \frac{d(U_j^a)}{dP_j} < 0 \quad (25)$$

hold. So there is one unique P_j^* , where $\frac{d^2(U_j^a)}{dP_j^2} = 0$, and this P_j^* is the unique
 255 optimal strategy for advertiser A_j when other advertisers' strategies are fixed. \square

Proposition 3 shows that when given other players' strategies P_{-j} , advertiser A_j has one unique optimal strategy P_j^* . As it is a non-cooperative game among advertisers, we next prove that in some situations Nash Equilibrium exists for
 260 this game, that is

Theorem 2. *When the total number of users N is large, there exists a strategy profile $P^* = (P_1^*, P_2^*, \dots, P_k^*)$, for which the following condition holds*

$$\forall j, P_j : U_j^a(P_j^*, P_{-j}^*) > U_j^a(P_j, P_{-j}^*). \quad (26)$$

Proof. The Gaussian error function $erf(x)$ can be approximated with elementary functions

$$erf(x) = 1 - \frac{1}{(1 + a_1x + a_2x^2 + \dots + a_6x^6)^{16}}, \quad (27)$$

where $\{a_i\}$ are approximate coefficients [22].

Then, we have

$$\begin{aligned} n_j &= N \int_0^{\frac{M_j}{\alpha_j}} f(\omega) d\omega \\ &= \frac{N}{2} \cdot \left[erf \left(\sqrt{\ln \frac{P_j N}{\alpha_j \sqrt{2\pi\sigma^2}}} \right) + erf \left(\frac{\mu}{\sqrt{2\sigma^2}} \right) \right] \\ &= \frac{N}{2} \cdot \left[2 - \frac{1}{(1 + a_1x + a_2x^2 + \dots + a_6x^6)^{16}} \right. \\ &\quad \left. - \frac{1}{(1 + a_1y + a_2y^2 + \dots + a_6y^6)^{16}} \right], \end{aligned}$$

where $x = \sqrt{\ln \frac{P_j N}{\alpha_j \sqrt{2\pi\sigma^2}}}$ and $y = \frac{\mu}{\sqrt{2\sigma^2}}$. As the total number of users N is large, $x > 1$. Note that we assume that $\mu > 3\sigma$ so that $y > \frac{3}{\sqrt{2}}$. Thus $n_j \rightarrow N$. The derivative of n_j with regard to P_j is

$$\frac{d(n_j)}{dP_j} = \frac{8N (a_1 + 2a_2x + 3a_3x^2 + \dots + 6a_6x^5)}{(1 + a_1x + a_2x^2 + \dots + a_6x^6)^{17}}. \quad (28)$$

And we have

$$\frac{d(n_j)}{n_j} = \frac{8 (a_1 + 2a_2x + 3a_3x^2 + \dots + 6a_6x^5)}{(1 + a_1x + a_2x^2 + \dots + a_6x^6)^{17}} \cdot dP_j. \quad (29)$$

As $x > 1$, $\frac{d(n_j)}{n_j} \rightarrow 0$. So when advertiser A_j changes its strategy, the change in the number of users who click the ad can be ignored, which means the optimal strategy of every advertiser does not change when other advertisers change their strategies. When all advertisers adopt their unique optimal strategies, their utilities are optimized, that is

$$\begin{aligned} \exists P^* &= (P_1^*, P_2^*, \dots, P_k^*) \\ \text{s.t. } \forall j, P_j &: U_j^a(P_j^*, P_{-j}^*) > U_j^a(P_j, P_{-j}^*). \end{aligned}$$

□

From the proof of the above theorem, we can easily derive the following proposition.

Proposition 4. *The optimal strategy of every advertiser does not change when other advertisers change their strategies.*

4.3. The Adoption of The Compensation Framework

The previous analyses have focused on analyzing the compensation framework under the advertiser-broker-user architecture, while our framework can be easily extended to the advertiser-user architecture, where advertisers directly deliver ads to users without the assistance of ad brokers. Our framework can be easily extended to this architecture. In this architecture, instead of paying fees to the ad broker, advertisers directly compensate users for their privacy loss.

To this end, we can simply set an extra constraint $\sum_j n_j P_j = \sum_j M_j$ in our
280 formulation. As such, all the fees paid by the advertisers $\sum_j n_j P_j$ become the
privacy loss compensation $\sum_j M_j$ paid to users.

The compensation framework motivates the users, advertisers and the ad
broker to participate in the targeted advertising system via economic incen-
tives. However, there may exist malicious entities whose target is not maximiz-
285 ing their utilities but trying to violate the rules defined by the compensation
framework. To cope with such cases, governments have made efforts to regulate
the behaviors of entities in online advertising. The White House has proposed
a Consumer Privacy Bill of Rights as part of a strategy to improve consumers
privacy protection, and has made an agreement with the Digital Advertising
290 Alliance, including Google, Yahoo!, Microsoft, etc., to regulate their advertising
behaviors [23]. The Advertising Regulation Department of Financial Industry
Regulatory Authority (FINRA) reviews broker-dealers' advertisements and oth-
er communications with the public to ensure that they are fair, balanced and
not misleading [24]. As such, the regulation from governments can ensure the
295 all parties follow the rules defined in the proposed compensation framework.

5. Numerical Results

In this section, we conduct extensive simulations to demonstrate the per-
formance gain of the proposed compensation framework, and the impact of the
system parameters on the performance.

300 5.1. Simulation Setup

We consider a system with 10^7 users, 50 advertisers and an ad broker, where
users are randomly allocated to 10 different preference profiles. A user is inter-
ested in an ad if the ad matches the user's profile [10]. Ads are delivered over
multiple time slots. In each time slot, an activity level, i.e., the fraction of users
305 that are active to view ads, is randomly chosen in $[0, 1]$. Unless explicitly other-
wise stated, privacy factor α is randomly distributed in $(0, 1)$, and the revenue

of each click $Q = 1$. The privacy factor α implies the relative content sensitivity of ads. An ad with larger α contains more sensitive content, and a user clicking it leaks more private information. An ad with $\alpha = 1$ refers to the ad containing the most sensitive content, while an ad with $\alpha = 0$ refers to the ad containing no sensitive information. Users' privacy sensitivities ω follow Gaussian distribution $N(\mu, \sigma^2)$ where $\mu = 1, \sigma = 0.01$. Recall that the users' privacy sensitivities ω is defined as the equivalent amount of compensation desired by the user for every unit of privacy loss. A user with larger ω values more about its private information, and thus needs stronger incentives to click sensitive ads.

To evaluate the performance gain of privacy-aware compensation, we compare our framework with the traditional paid-to-click (PTC) model, which is a popular online business model that motivates users to view ads. In the traditional PTC model, a certain price is paid to users for every click, while the diversities of ad content and user's sensitivity are not considered. For fair comparison, we enhance the PTC model by implementing it in our privacy-aware setting. In particular, the enhanced PTC model employs a privacy dependent pricing scheme where click price is determined optimally according to the user's privacy sensitivity.

5.2. Results

We first evaluate the overall performance of our framework by comparing it with the PTC model in Section 5.2.1. Then, we evaluate our framework under various settings of privacy related parameters, i.e., the privacy factor α and user's privacy sensitivity ω in Section 5.2.2. Finally, we study the impact of competition among advertisers in Section 5.2.3.

5.2.1. Comparison of Different Frameworks

We first show the overall merits of the proposed compensation framework by comparing it with the traditional PTC framework. To show that our framework can incentivize different kinds of users, that is, users with different sensitivities, we vary the average privacy sensitivity μ . In particular, we compare the number

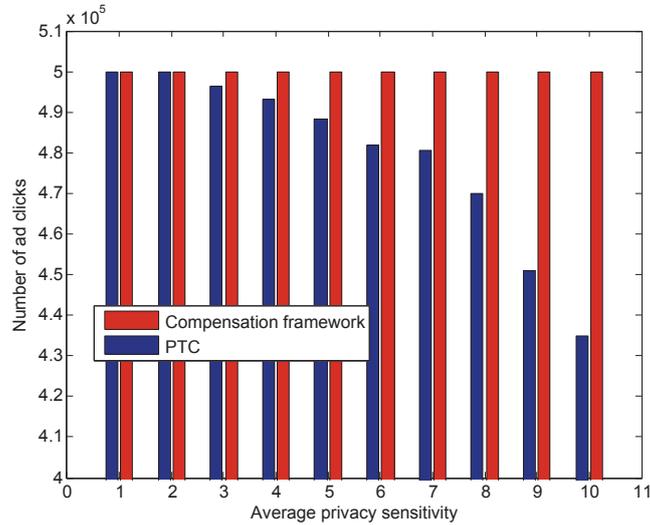


Figure 3: Number of ad clicks versus average privacy sensitivity.

of ad clicks, the revenue of advertisers, and the revenue of the ad brokers in Figure 3, Figure 4, and Figure 5, respectively.

Comparing the number of ad clicks achieved by different frameworks. Figure 3 compares the number of ad clicks for users with different levels of privacy concerns. Number of ad clicks, which determines click-through rate, is considered as an essential indicator for the efficiency of advertising. In all cases demonstrated, the number of ad clicks achieved by the compensation framework is larger than that in the PTC framework, which means that our framework outperforms the PTC in terms of the efficiency of advertising. The number of ad clicks decreases with average privacy sensitivity under the PTC framework, but remains almost unchanged under the compensation framework. This is because the PTC framework pays users based a unified pricing model, while the compensation policy considers the privacy loss of different users and is tailored to different ads, which can motivate more users.

Comparing the revenue of advertisers achieved by different frameworks. Figure 4 shows that when the average privacy sensitivity increases, the revenue of

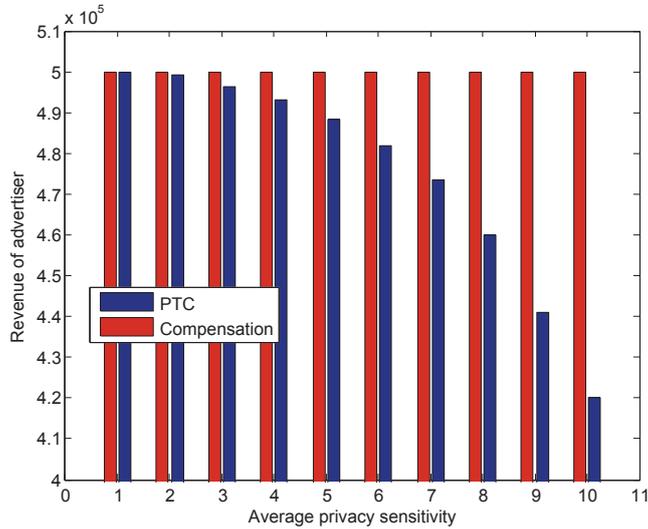


Figure 4: Revenue of advertisers versus average privacy sensitivity.

advertisers drops significantly under the PTC framework, while the advertisers under the compensation framework still maintains their revenue at a high level, which implies that the proposed compensation framework successfully incentivizes highly sensitive users and brings more revenues to advertisers. The trends of advertisers' revenue are consistent with the trends of number of ad clicks as depicted in Figure 3. The reason is that the revenue of advertisers is much determined by the number of ad clicks. It is indicated in equations (11) and (15) that when the shape of distribution $f(\omega)$ does not change, the relationship between n_j and P_j stays the same. Advertiser A_j 's revenue is only affected by Q_j , n_j and P_j , where Q_j is a constant number, so that its strategy remains the same with the increase in μ , which in turn makes n_j and advertiser's profit constant. The results of Figure 4 further validate that the compensation framework brings more profits to advertisers.

Comparing the revenue of the ad broker achieved by different frameworks. Figure 5 illustrates the revenue of the ad broker with different level of average privacy sensitivity. In all cases demonstrated, the compensation framework

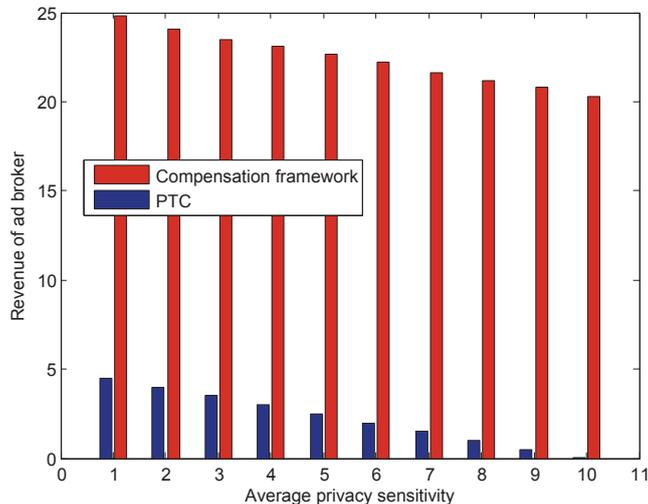
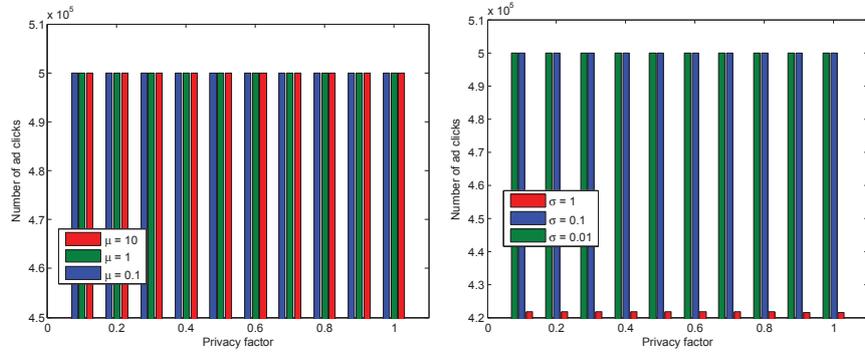


Figure 5: Revenue of the ad broker versus average privacy sensitivity.

brings considerably more revenue to the ad broker compared to the PTC frame-
work, which indicates that the compensation framework can better motivate
370 the ad broker to involve the advertising systems. With higher average privacy
sensitivity, the performance gain of the compensation framework is larger. The
reason is that in our framework, the amount of compensation is tailored to each
click according to the ad content and user’s sensitivity, and leads to more ad
clicks, which makes advertisers pay more to the ad brokers. An interesting ob-
375 servation is that the revenues of the ad broker decrease under both frameworks
with higher privacy sensitivity. This is because the price to compensate user’s
privacy loss is higher for high sensitive users. As such, a larger portion of the
ad broker’s income is used to motivate users.

5.2.2. Impact of Privacy Parameters

380 In this subsection, we evaluate the proposed compensation framework under
various privacy settings. In particular, we show how privacy factor of an ad and
user’s privacy sensitivity affect the revenues of advertisers and the ad broker.
In Figure 6-9, we vary the privacy factor α of each ad from 0.1 to 1, and select



(a) Varying the mean of users' privacy sensitivities (b) Varying the standard deviation of users' privacy sensitivities

Figure 6: Number of ad clicks.

different values of the mean and standard deviation of user's privacy sensitivity.

385 **The number of clicks under various privacy settings.** Figure 6 reports the number of clicks achieved by the compensation framework with different values of privacy factor α and distributions of privacy sensitivity. The privacy factor of an ad determine the privacy level of an ad and the privacy loss of an click. The compensation amount is adjusted according to each ad's privacy factor to stimulate users. It can be seen that the number of ad clicks stay unchanged with different values of privacy factor, which demonstrate the effectiveness of the stimulation for different kinds of ads. In Figure 6(a), we observe that the value of μ has little impact on the number of clicks, which is consistent with the results shown in Figure 3. Figure 6(b) shows that when the standard deviation of users' privacy sensitivity varies from 0.1 to 1, the number of ad clicks declines. When the the standard deviation of users' privacy sensitivity is large, it costs more for the advertisers and the ad broker to incentive users, as analyzed in Section 4. As such, less compensation is allocated to users, resulting in less ad clicks. This observation reveals that for users with very diverse privacy sensitivities, it is more effective to categorize users according to their privacy sensitivity and employ dedicated strategy for each category.

390
395
400

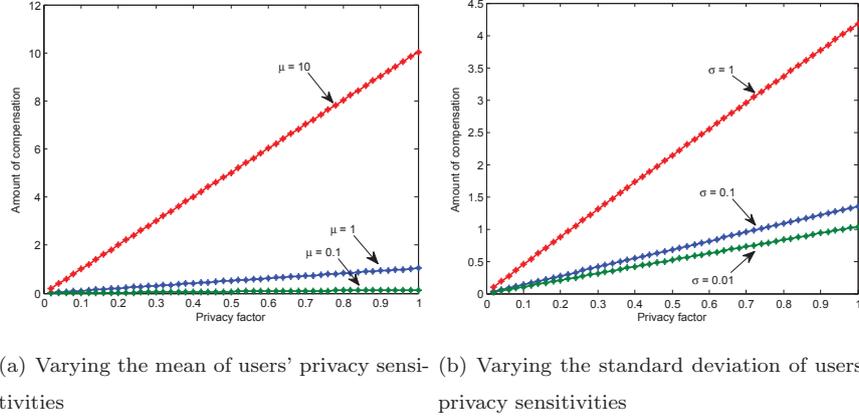
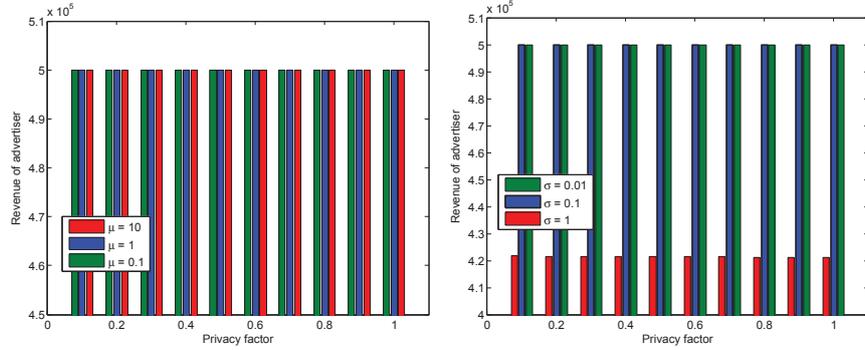


Figure 7: Amount of compensation.

The amount of compensation under various privacy settings. The amount of compensation is an important factor that affects the revenue of the ad broker. We study the amount of compensation in Figure 7. The amount of compensation grows with privacy factor, as the ad broker needs to pay more to stimulate users to click ads of higher privacy factor. For larger μ and σ , the average privacy loss for users with privacy sensitivity higher than μ is larger, which determines larger amount of compensation to motivate users.

The revenues under various privacy settings. Figure 8 depicts the revenue of advertisers against the privacy factor and privacy sensitivity. The results are consistent with Figure 6 as the number of clicks largely determines the revenue of advertisers. An interesting observation in Figure 8(b) is that the revenue of advertisers diminishes as the standard deviation of privacy sensitivity increases. With larger standard deviation of privacy sensitivity, advertisers have the incentive to increase its offer to encourage the ad broker to pay more to users. As analyzed in Section 4, the optimal point is on the right half of the probability distribution function, which means that advertisers and the ad brokers are more concerned about 50% of the users whose privacy sensitivities are higher than average, as the other half are always stimulated to click. With the increment of



(a) Varying the mean of users' privacy sensi- (b) Varying the standard deviation of users' tivities privacy sensitivities

Figure 8: Revenue of advertisers.

420 the standard deviation, the privacy sensitivity level of the “concerned group” is rising so that both advertisers and the ad broker raise their offers.

Figure 9 shows the impact of privacy factor and the privacy sensitivity on the revenue of the ad broker. An counter-intuitive observation is that the revenue of the ad broker grows with privacy factor. This is because the payment from
 425 advertisers dominates the revenue of the ad broker, and for ads with higher privacy factor, advertisers tend to pay more to motivate the ad broker to allocate more compensation to users. Combining the results in Figure 7 and Figure 9, we find that although larger μ and σ lead to more compensation, while the revenue of the ad broker diverges in such two cases: the revenue of the ad broker declines
 430 with larger μ , but increases with larger σ . The reason is that as μ increases, advertisers maintain a constant profit as shown in Figure Figure 8(a), and it is the ad broker who pays for the users' higher privacy loss; while as σ grows, users with more diverse privacy sensitivities make advertisers pay more to the ad broker to indirectly motivate users, as discussed earlier.

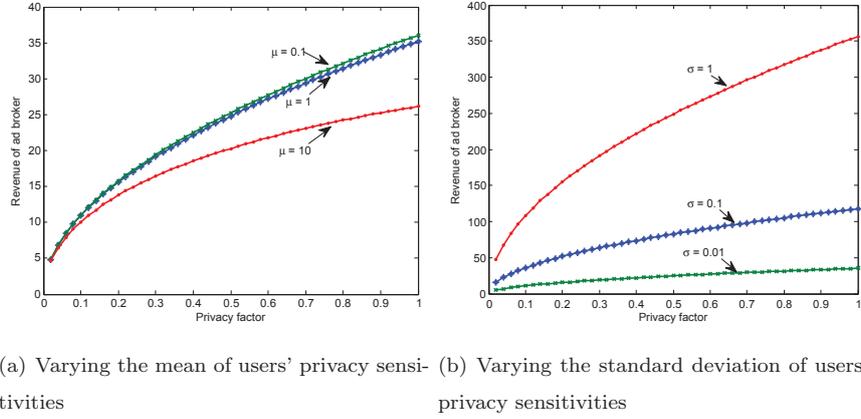


Figure 9: Revenue of ad broker.

435 *5.2.3. Impact of Competition Among Advertisers*

Note that the above evaluations focus on independent advertisers, e.g., advertisers for irrelevant contents. Next we discuss how the competition among advertisers affect their decisions and revenues. In the competition model, advertisers deliver similar ads and share one market. In this subsection, we present the simulation results of the scenario where there are two similar advertisers sharing one market, which can be easily visualized.

First, we study the case where both advertisers deliver ads of the same privacy factor, which is set to be 1. Figure 10 shows the impact of both advertisers' strategies, i.e. the price of every click, on advertiser 1's revenue. The results show that advertiser 2's price has little impact on advertiser 1's optimal price, which verifies our theoretical results in Proposition 4.

Then, we study the case where advertisers deliver ads of very different privacy factors. We set the privacy factor of ad 2 as 30 while ad 1's remains at 1. Recall that the privacy factor of an ad implies its content sensitivity. As such, ad 2 is much more sensitive than ad 1. Figure 11 shows that although the revenue of advertiser 1 no longer keeps constant when the price of advertiser 2 changes as Figure 10 shows, the optimal price of advertiser 1 maintains constant, which

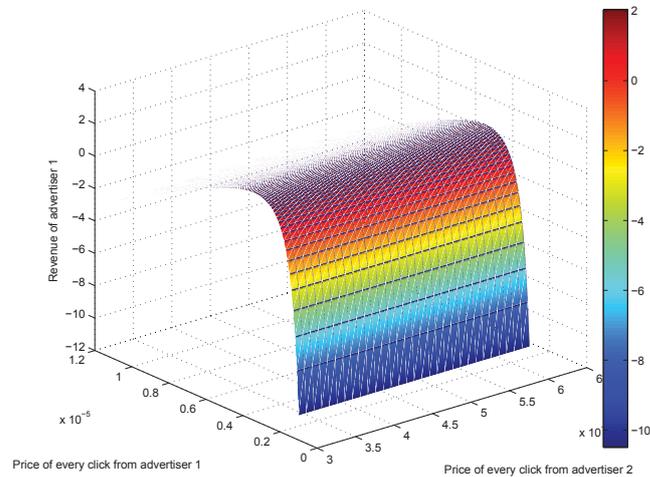


Figure 10: Revenue of advertisers with the same privacy factor. Privacy factors for both advertisers' ads are 1.

demonstrates that the Nash Equilibrium can also be achieved when different ads have different privacy factors. Another observation from Figure 11 is that
 455 the revenue of advertiser 1 decreases with the increment of advertiser 2's price. This is because advertisers are competing with each other, advertiser 1 loses its user when advertiser 2 offers higher price.

6. Related Work

Existing studies related to privacy-aware targeted advertising can be classi-
 460 fied into three categories: targeted advertising mechanisms, privacy preservation on user's online profiles or behaviors, and incentive mechanism designs for advertising and trading privacy.

Targeted Advertising Mechanisms. Targeted advertising mechanisms
 465 mainly focus on the strategies of advertisers or the ad broker to deliver ads to matched users. Chakrabarti et al. [25] studies the problem of displaying relevant ads to web pages and proposes a new class of models to combine relevance

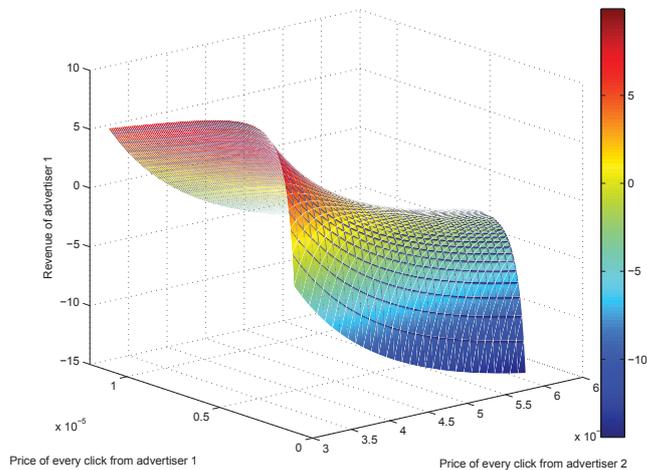


Figure 11: Revenue of advertisers with very different privacy factor. Privacy factors for advertiser 1' ads and advertiser 2's ads are 1 and 30, respectively.

and click feedback for contextual advertising. Mechanisms for search engine to match ads with queries are discussed in [26, 27, 28]. These studies model the interactions between the ad broker and advertisers as an auction problem, in which advertisers bid for ads displayed on the search results pages. Provost
 470 et al. [29] study the problem of targeted advertising in the context of social networks, and introduce a framework to select users based on page visitations. These works have focused on the strategies of advertisers and the ad broker, while our framework take into account the impact of user behaviors on targeted
 475 advertising.

Privacy Preservation. Many recent works have investigated privacy issues in user's online profiles and behaviors, which are involved in targeted advertising. Privad [9] keeps the users' profile at their local devices, and introduces an anonymizer sitting between users and the ad broker to anonymize user's click-
 480 s. Kodialam et al. [10] propose a targeted advertising system in which users are allowed to send perturbed click statistics to preserve privacy. Adnostic [8]

offloads the ad broker’s task, i.e., behavioral profiling and targeting, to user’s local browser. **Privad [16] introduce an extra proxy to preserve user’s privacy.** These privacy-preserving systems protect user’s privacy at the cost of advertisers’ or the ad broker’s interests, and ignore their incentives to promote such systems. Our compensation framework is built based on their basic privacy-preserving architecture, that is, keeping users’ profile at local devices, and aims to fill the gap between user’s privacy protection and the economic incentives of advertisers and the ad broker. There are also many privacy preserving techniques for user’s online behaviors [30, 31, 32]. These techniques normally perturb user’s actions to hide their precise behaviors, which, however, cannot be directly applied to the targeted advertising as precise clicking information is a prerequisite to determine advertiser’s payment.

Incentive Mechanism Design. Several incentive mechanisms are proposed for advertising and trading user’s private data. Ning et al. [33] formulate the ad forwarding problem in delay-tolerant networks as a two-player cooperative game, and devise an incentive scheme to motivate users to forward ads. The privacy-aware mechanism was first proposed in [12] to include the valuation of privacy as a part of player’s utility. Ghosh et al. [13] consider privacy as a commodity, and derive truthful auctions for private data trading. Our framework is inspired by these studies. Nevertheless, they are different from the targeted advertising problem studied in this paper, where all advertisers, users, and the ad broker are decision makers, and their interactions are modeled and analyzed through different stages.

505 7. Conclusion

This paper has studied the privacy-aware targeted advertising problem, and proposed a compensation framework to encourage users to view ads of interest. The compensation framework aims to promote targeted advertising by creating a win-win situation. Under this framework, we analyze the interactions among 510 advertisers, the ad broker, and users through a three-stage game modeling. Sim-

ulation results demonstrate the efficacy of the proposed framework, under which users are motivated to click more interested ads and both the advertiser and the ad broker achieve considerable gains in their revenues. Therefore, with proper design, the compensation framework can promote the adoption of targeted advertising and bring merits for all entities.

Acknowledgement

The research was support in part by grants from 973 project 2013CB329006, China NSFC under Grant 61173156, RGC under the contracts CERG 622613, 16212714, HKUST6/CRF/12R, and M-HKUST609/13, as well as the grant from Huawei-HKUST joint lab.

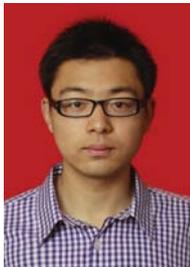
References

- [1] J. Yan, N. Liu, G. Wang, W. Zhang, Y. Jiang, Z. Chen, How much can behavioral targeting help online advertising?, in: Proc. ACM WWW, 2009.
- [2] W. Wang, Q. Zhang, A stochastic game for privacy preserving context sensing on mobile phone, in: Proc. IEEE INFOCOM, 2014.
- [3] H. Beales, The value of behavioral targeting, in: Network Advertising Initiative, 2010.
- [4] Google adwords, <http://www.google.com/ads/adwords/>.
- [5] Ink tad, <http://www.ink-global.com/what-we-do/tad/>.
- [6] K. Purcell, J. Brenner, L. Rainie, Search engine use 2012, in: Pew Internet & American Life Report, 2012.
- [7] J. Turow, J. King, C. J. Hoofnagle, A. Bleakley, M. Hennessy, Americans reject tailored advertising and three activities that enable it, in: SSRN, 2009.

- 535 [8] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, S. Barocas, Ad-
nastic: Privacy preserving targeted advertising, in: Proc. NDSS, 2010.
- [9] S. Guha, B. Cheng, P. Francis, Privad: practical privacy in online adver-
tising, in: Proc. NSDI, 2011.
- [10] M. Kodialam, T. Lakshman, S. Mukherjee, Effective ad targeting with
540 concealed profiles, in: Proc. IEEE INFOCOM, 2012.
- [11] V. Dave, S. Guha, Y. Zhang, Measuring and fingerprinting click-spam in
ad networks, in: Proc. ACM SIGCOMM, 2012.
- [12] K. Nissim, C. Orlandi, R. Smorodinsky, Privacy-aware mechanism design,
in: ACM Proc. EC, 2012.
- 545 [13] A. Ghosh, A. Roth, Selling privacy at auction, Elsevier Games Econ. Behav.
(2013).
- [14] L. Yang, W. Wang, Y. Chen, Q. Zhang, A privacy-aware framework for
online advertisement targeting, in: Proc. IEEE GLOBECOM, 2013.
- [15] S. Clifford, Web startups offer bargains for users data, in: The New York
550 Times, 2010.
- [16] H. Haddadi, S. Guha, P. Francis, Not all adware is badware: Towards
privacy-aware advertising, in: Springer Software Services for e-Business
and e-Society, 2009, pp. 161–172.
- [17] S. Majumdar, D. Kulkarni, C. V. Ravishankar, Addressing click fraud in
555 content delivery systems, in: Proc. IEEE INFOCOM, 2007.
- [18] H. Haddadi, Fighting online click-fraud using bluff ads, ACM SIGCOMM
Computer Communication Review 40 (2) (2010) 21–25.
- [19] L. Sweeney, k-anonymity: A model for protecting privacy, International
560 Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10 (05)
(2002) 557–570.

- [20] D. W. Bedford, Empirical investigation of the acceptance and intended use of mobile commerce: location, personal privacy and trust, Mississippi State University, 2005.
- [21] W. Wang, Q. Zhang, Privacy-preserving collaborative spectrum sensing with multiple service providers, *IEEE Trans. Wireless Commun.* PP (99) (2014) 1–8.
- [22] M. Abramowitz, I. A. Stegun, Handbook of mathematical functions: with formulas, graphs, and mathematical tables, Courier Dover Publications, 2012.
- [23] D. Weitzner, Obama administration calls for a consumer privacy bill of rights for the digital age.
- [24] Finra’s advertising regulation.
URL <http://www.finra.org/Industry/Issues/Advertising/>
- [25] D. Chakrabarti, D. Agarwal, V. Josifovski, Contextual advertising by combining relevance with click feedback, in: *Proc. ACM WWW*, 2008.
- [26] A. Mehta, A. Saberi, U. Vazirani, V. Vazirani, Adwords and generalized online matching, *J. ACM* 54 (5) (2007) 1–22.
- [27] N. Devanur, T. Hayes, The adwords problem: online keyword matching with budgeted bidders under random permutations, in: *Proc. ACM EC*, 2009.
- [28] N. Buchbinder, K. Jain, J. S. Naor, Online primal-dual algorithms for maximizing ad-auctions revenue, in: *Algorithms–ESA*, Springer, 2007.
- [29] F. Provost, B. Dalessandro, R. Hook, X. Zhang, A. Murray, Audience selection for on-line brand advertising: privacy-friendly social network targeting, in: *Proc. ACM SIGKDD*, 2009.

- [30] F. G. Mármol, J. Girao, G. M. Pérez, Trims, a privacy-aware trust and reputation model for identity management systems, Elsevier Computer Networks 54 (16) (2010) 2899–2912.
- [31] C. Rottondi, G. Verticale, A. Capone, Privacy-preserving smart metering with multiple data consumers, Elsevier Computer Networks 57 (7) (2013) 1699–1713.
- [32] F. Tschorsch, B. Scheuermann, An algorithm for privacy-preserving distributed user statistics, Elsevier Computer Networks 57 (14) (2013) 2775–2787.
- [33] M. Kodialam, T. Lakshman, S. Mukherjee, Self-interest-drive incentives for ad dissemination in autonomous mobile social networks, in: Proc. IEEE INFOCOM, 2013.



Wei Wang is currently a Ph.D. candidate in Hong Kong University of Science and Technology. He received his B.E. degree in Electronics and Information Engineering from Huazhong University of Science and Technology, Wuhan, China, in 2010. His research interests include privacy, fault management and PHY/MAC design in wireless networks.



Linlin Yang is currently a M.Phil. student in Hong Kong University of Science and Technology. She received her B.E. degree of electronic engineering from Tsinghua University in 2012. Her research interests include privacy protection for advertising and network economics.



Yanjiao Chen received her B.E. degree of electronic engineering from Tsinghua University in 2010. She is currently a Ph.D. candidate in Hong Kong University of Science and Technology. Her research interests include spectrum management for Femtocell networks and network economics.



Qian Zhang joined Hong Kong University of Science and Technology in Sept. 2005 where she is a full Professor in the Department of Computer Science and Engineering. Before that, she was in Microsoft Research Asia, Beijing, from July 1999, where she was the research manager of the Wireless and Networking Group. Dr. Zhang has published about 300 refereed papers in international leading journals and key conferences in the areas of wireless/Internet multimedia networking, wireless communications and networking, wireless sensor networks, and overlay networking. She is a Fellow of IEEE for “contribution to the mobility and spectrum management of wireless networks and mobile communications”. Dr. Zhang has received MIT TR100 (MIT Technology Review) worlds top young innovator award. She also received the Best Asia Pacific (AP) Young Researcher Award elected by IEEE Communication Society in year 2004. Her current research is on cognitive and cooperative networks, dynamic spectrum access and management, as well as wireless sensor networks. Dr. Zhang received the B.S., M.S., and Ph.D. degrees from Wuhan University, China, in 1994, 1996, and 1999, respectively, all in computer science.