How Good Are Privacy Guarantees? Platform Architecture and Violation of User Privacy

Daron Acemoglu [*] Alireza Fallah [†] Ali Makhdoumi [‡] Azarakhsh Malekian [§]
Asuman Ozdaglar [†]

June 18, 2023

Abstract

Many platforms deploy data collected from users for a multitude of purposes. While some are beneficial to users, others are costly to their privacy. The presence of these privacy costs means that platforms may need to provide guarantees about how and to what extent user data will be harvested for activities such as targeted ads, individualized pricing, and sales to third parties. In this paper, we build a multi-stage model in which users decide whether to share their data based on privacy guarantees. We first introduce a novel *mask-shuffle* mechanism and prove it is Pareto optimal—meaning that it leaks the least about the users' data for any given leakage about the underlying common parameter. We then show that under any mask-shuffle mechanism, there exists a unique equilibrium in which privacy guarantees balance privacy costs and utility gains from the pooling of user data for purposes such as assessment of health risks or product development. Paradoxically, we show that as users' value of pooled data increases, the equilibrium of the game leads to lower user welfare. This is because platforms take advantage of this change to reduce privacy guarantees so much that user utility declines (whereas it would have increased with a given mechanism). Even more strikingly, we show that platforms have incentives to choose data architectures that systematically differ from those that are optimal from the user's point of view. In particular, we identify a class of pivot mechanisms, linking individual privacy to choices by others, which platforms prefer to implement and which make users significantly worse off.

1 Introduction

Online platforms have proliferated over the last two decades, and many of them now obtain a significant part of their revenue from harvesting user data. Users directly benefit from some of the activities enabled by data collection. For example, they receive better recommendations or

[*]Department of Economics, Massachusetts Institute of Technology
[†]Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology
[‡]Fuqua School of Business, Duke University
[§]Rotman School of Management, University of Toronto.

customization for products or services, and pooled data are deployed for learning about health conditions for the population, their group, or directly for themselves. Yet, other data-intensive activities, such as targeted digital ads, individualized pricing, and data sales to third parties, may be costly, annoying, or privacy-violating for users. The willingness of users to share their data typically depends on guarantees that there will be limits to these practices that are costly to them.

In this paper, we build a model to study these issues. We consider a set of users who have a utility consisting of two terms. The first attaches a positive value, with weight α, to the precision of society's (or the platform's) estimate of an underlying common state, θ, based on pooled user data. The second attaches a negative value, with weight β, to the decline in the mean squared error about the individual's own type, which is used by the platform for pricing or ad targeting. For concreteness, we could consider the state θ to correspond to the prevalence of a virus in the population, such as COVID- 19, while the individual type may be whether the user herself has been infected, which she may wish to keep private. We assume that the platform receives positive returns from acquiring more information on both components.

The key decision for users is whether to share their data (or participate in the platform). If the potential cost of privacy violations is large enough, they will choose not to do so, unless adequate privacy guarantees are provided by the platform.

The game between the platform and the users is conceptualized as follows. First, the platform commits to a mechanism for partially preserving user privacy. Second, users decide individually whether to share their data. Then the platform uses the data according to the chosen mechanism, and utilities are realized. We look for a (Bayesian) Stackelberg equilibrium of this game, whereby the platform optimally chooses the mechanism, anticipating the following Bayesian Nash equilibrium.

What makes this game interesting and difficult is the fact that the space of mechanisms that provide privacy guarantees is vast, including partial anonymization, limits on what data can be used for, various ways of adding noise to the data, and differential privacy and related mechanisms.

Formally, we define a mechanism as a mapping from the users' data to an output and consider the following pair of quantities in the space of *all possible mechanisms*: leaked information about the underlying common parameter and the sum of leaked information about each user's private data. We then ask the following question:

> *In the space of all mechanisms, is there a mechanism that achieves the Pareto frontier (i.e., leaks the most about the underlying common parameter and the least about users' data)? What is that mechanism?*

One of our main results is that a *mask-shuffle mechanism* achieves the Pareto frontier defined above. This proves that from the viewpoint of the users, this mechanism provides the optimal trade-off between the positive and the negative uses of data. Specifically, according to this optimal mechanism, the platform should commit to a probability with which a user's data will be fully

anonymized (will be shuffled across users). This type of mask-shuffle is attractive from the users' viewpoint because it maintains information about the underlying state but implies that the platform learns much less about the individual. By choosing the probability of shuffling, the platform can fine-tune the privacy guarantees to users.

Our second result characterizes the (unique and Bayesian) Stackelberg equilibrium under any mask-shuffle mechanism. Additionally, we provide a number of comparative statics of this equilibrium, showing how the extent to which users and the platform care about privacy affects the degree of anonymity. Our comparative statics is more subtle and surprising, highlighting the paradox of platform-provided privacy guarantees. When α (the weight attached to the positive use of pooled data in order to learn the state θ) increases, user utility increases given any mask-shuffle mechanism, and users become more willing to share their data so that it can be pooled with those of others to obtain better estimates of θ. Greater α, however, also means that the platform now chooses lower privacy guarantees. The paradoxical result is that this platform response is powerful enough that, under some conditions we characterize, users end up worse off than they would have been with lower α. We interpret this result as suggesting that platform-provided privacy guarantees are highly imperfect and often insufficient.

Our final result turns to the implications of user privacy preferences on platform choices of data architecture. We prove that the platform has an incentive to deviate from the user-optimal mask-shuffle mechanisms. In particular, we identify a set of *pivot mechanisms* that make individual privacy on the choices of other users, for example, by linking the decision of how much of a user's data to utilize on the sharing decision of other users. We establish that the platform can exploit user preferences towards the underlying common state, θ, by designing a pivot mechanism that commits to not utilizing any user data if any one of the users does not share her data. This pivot mechanism makes every user "pivotal" at the margin, meaning that if she decides not to share her data, nothing is learned about θ. Because the user values social learning about θ, the effective cost of not sharing her data increases significantly, and this allows the platform to violate her privacy. We also show that more continuous versions of pivot mechanisms can achieve the same outcome. This result further amplifies our interpretation that self-regulation by platforms is often insufficient to ensure sufficient user privacy.

1.1 Related literature

Our paper relates to a large and growing literature on privacy. Several papers consider the design of mechanisms for collecting data from privacy-aware users, including Ghosh and Roth [2011], Ligett and Roth [2012], Nissim et al. [2014], Cummings et al. [2015], Chen et al. [2018], Chen and Zheng [2019], and Fallah et al. [2022a]. For example, Ghosh and Roth [2011] study a setting in which each user has a private bit and a heterogeneous privacy loss parameter and the platform wants to design a dominant strategy truthful mechanism to learn the sum of user's data. On the other hand, Cummings et al. [2015] consider a model in which users charge the platform based on the accuracy level of the data that they provide, and the platform decides on the level of accu-

racy that she purchases. Finally, Fallah et al. [2022a] and Fallah et al. [2022b] focus on designing Bayesian optimal schemes to collect data from strategic users with heterogeneous privacy sensitivities under local and central privacy architectures. We differ from these papers by explicitly modeling the game between the platform and users, and we focus on a setting in which there are no explicit prices, but the costs and benefits of the services provided by the platform have to convince users to take part in data sharing. Specifically, in our model, as in Cummings et al. [2022] and Fallah et al. [2022a], users benefit from the quality of the estimate about the underlying state. However, these papers do not study the design of optimal platform mechanisms with strategic users, either.[1]

Even more closely related is the emerging literature on the social dimension of data and online platform behavior, for example, Acemoglu et al. [2022] and Bergemann et al. [2020]. Bergemann et al. [2020] consider a setting in which a (trusted) data intermediary collects users' data and resells them to a platform. They show that data externalities, whereby a user's data is predictive of others, can reduce the intermediary's cost of acquiring the data. Acemoglu et al. [2022] consider a more general, though reduced-form, data externality and establish that this externality reduces the value of data to both users and the platform. As a result, data externalities depress data prices and amplify inefficiencies. Relatedly, Ichihashi [2020] studies the interactions between a privacy-concerned user and a platform, where the user's activity reveals private information (see also Fainmesser et al. [2022] for a similar model). These papers do not consider general privacy-preserving mechanisms.

More broadly, our work is also related to the literature on data collection and sharing. Hörner and Skrzypacz [2016] study the design of mechanisms for selling data, while Goldfarb and Tucker [2011], Bergemann and Bonatti [2015], Montes et al. [2019], and Jagabathula et al. [2020] investigate how individual private information can be used to improve resource allocation. Competition implications of online data sharing and technologies have been explored in, among others, Bimpikis et al. [2021] and Gur et al. [2019]. Bergemann and Bonatti [2015] study the problem of selling cookies for targeted advertisement and study how the price of data changes with the reach of the dataset and the fragmentation of data sales. Fu et al. [2022] study data collection and privacy in recommendation systems. Other works on information-sharing and market structure include Li [2002], Li and Zhang [2008], Ha and Tong [2008], Shang et al. [2015], Foster et al. [2016], Lobel and Xiao [2017], Bimpikis et al. [2019], Candogan and Drakopoulos [2020], Immorlica et al. [2020], Hu et al. [2020], Ashlagi et al. [2020], Anunrojwong et al. [2021], Besbes and Mouchtaki [2021], and Ashlagi et al. [2021] (see Bergemann and Bonatti [2019] for a survey).

The rest of the paper proceeds as follows. Section 2 presents the users' and the platform's utility and establishes the optimality of the mask-shuffle mechanism. In Section 3, we introduce the equilibrium concept and establish its existence. In Section 4, we characterize the equilibrium of the game among the users and the platform and provide some comparative statics for it. In

[1]Motivated by applications in which users grant permission to use their data to platforms, we do not consider the issue of misreporting of data. The issue of misreporting is studied in Perote and Perote-Pena [2003], Dekel et al. [2010], Meir et al. [2012], Ghosh et al. [2014], Cai et al. [2015], and Liu and Chen [2016, 2017], among others.

Section 5, we establish that the platform has incentives to use mechanisms other than mask-shuffle as opposed to the users. Section 6 concludes, while the Appendix presents the omitted proofs.

2 Environment

We consider a platform that wishes to collect data from n privacy-aware users denoted by $\mathcal{N} = \{1, \dots, n\}$. User i's data is represented by $X_i = \theta + Z_i$ where $\theta \sim \mathcal{N}(0,1)$ is a common parameter and $Z_i \sim \mathcal{N}(0,1)$ is user i's private type. We assume both users and the platform drive higher utility from having access to a better estimation of θ. The private type of user i, Z_i, can be used for the platform's benefit, and therefore the platform gains from a better estimation of it while the user suffers a privacy loss. Users and the platform connect through a **mechanism**. Formally, a mechanism $\mathcal{M} : \mathbb{R}^n \to \mathcal{X}$, for some set $\mathcal{X}$, is a randomized algorithm whose input is the users' data, i.e., $x_1, \cdots, x_n$, and its output is received by the platform. The mechanism output is used by the platform to estimate θ. The mechanism output contains information about the underlying parameter θ which leads to a better estimation of this parameter and benefits both the users and the platform. It also reveals information about the private type of users z_i for $i \in \mathcal{N}$ which benefits the platform but harms the users.

Before introducing the utility of the users and the platform we introduce our measure of *revealed information*. Throughout the paper, we use lower case letters to denote the realization of random variables. Notice that platform's prior on θ and Z_i is $\pi_0 = \mathcal{N}(0,1)$. We denote the platform's posterior on θ and Z_i after observing the mechanism's output by $\pi_\theta(\mathcal{M})$ and $\pi_{Z_i}(\mathcal{M})$, respectively. It can be seen that the best estimator of θ and Z_i's with respect to the mean-squared error, given the mechanism's output, is the mean of the posterior distributions. We define revealed information as the reduction in the mean-squared error from the prior to the posterior, formalized next.[2]

Definition 1 (Revealed information)**.** *For any mechanism $\mathcal{M}$, revealed information about θ is the reduction in the mean-squared error of θ, i.e.,*

$$\mathcal{I}(\theta \mid \mathcal{M}) = \mathbb{E}\left[\left(\theta - \mathbb{E}_{\theta\sim\pi_0}[\theta]\right)^2\right] - \mathbb{E}\left[\left(\theta - \mathbb{E}_{\theta\sim\pi_\theta(\mathcal{M})}[\theta]\right)^2\right],$$

where the expectations are over the randomness in data and the mechanism. Similarly, for any $i \in \mathcal{N}$, revealed information about Z_i is the reduction in the mean-squared error of Z_i, i.e.,

$$\mathcal{I}(Z_i \mid \mathcal{M}) = \mathbb{E}\left[\left(Z_i - \mathbb{E}_{Z_i\sim\pi_0}[Z_i]\right)^2\right] - \mathbb{E}\left[\left(Z_i - \mathbb{E}_{Z_i\sim\pi_{Z_i}(\mathcal{M})}[Z_i]\right)^2\right].$$

Given the above definition of revealed information, the expected **utility of user** i is given by

$$\mathcal{U}_i(\mathcal{M}) := \alpha\, \mathcal{I}(\theta \mid \mathcal{M}) - \beta\, \mathcal{I}(Z_i \mid \mathcal{M}). \tag{1}$$

[2] In our setting, privacy is ensured when the disclosed information, as defined below, is small. This guarantee is based on an average-case scenario, which differs from the worst-case guarantees provided by differential privacy Dwork et al. [2014].

The first term captures the gain of user i from a better estimation of the underlying parameter θ. For instance, in the context of a medical study, the user gains from a better estimation by the hospital, leading to a more effective drug. The second term captures the loss of learning user i's private data Z_i. Again, in the context of a medical study, the user wants to keep her medical record private. We use parameters α and β that are non-negative as constants to scale the impact of learning the underlying parameter and the user's private data, respectively. In the context of a medical study, again, they capture the relative weight that users assign to a more effective drug versus their privacy loss. The expected **platform's utility** is given by

$$\mathcal{U}_{\text{platform}}(\mathcal{M}) := \mathcal{I}(\theta \mid \mathcal{M}) + \delta \sum_{i=1}^{n} \mathcal{I}(Z_i \mid \mathcal{M}), \tag{2}$$

where the first and second terms correspond to the platform's gain from learning θ and users' private type, respectively. Notice that, without loss of generality, we have normalized the impact of learning θ in platform's utility to one and use a non-negative constant δ to scale the impact of learning users' private data in the platform's utility.

2.1 Mask-shuffle mechanism and its optimality

The space of mechanisms includes all possible mappings from users' data to an arbitrary space. In principle, this class includes a rich set of mechanisms. Nevertheless, we now establish that user-optimal mechanisms take a relatively simple form, which we call *mask-shuffle mechanisms*. In particular, we prove that the mask-shuffle mechanism achieves the minimum sum of revealed information about private user types, the Z_i's, for a given revealed information about θ.

Definition 2 (Mask-shuffle mechanism)**.** *A mask-shuffle mechanism is a pair* $(\mathbf{q}, \mu) \in [0,1]^{n+1}$ *such that:*

1. *The data of each user* $i \in \mathcal{N}$ *is completely hidden from the platform with probability* $1 - q_i$ *(denoted by NA) and is kept with probability* q_i*.*

2. *Letting* Y_i *denote the user* i*'s data after this randomized mapping, the mechanism directly releases each* Y_i *with an independent probability* $1-\mu$ *and shuffles the rest and releases a permutation of these shuffled* Y_i*'s (i.e.,* $Y_{i_{\sigma(1)}}, \ldots, Y_{i_{\sigma_k}}$ *for some random permutation* σ *where* k *is the number of* Y_i*'s that are shuffled).*

Figure 1a illustrates the mask-shuffle mechanism that includes a partial shuffler that shuffles each user's data with probability μ. Figure 1b further depicts this partial shuffling element.

Before establishing the optimality of a mask-shuffle mechanism, we explicitly characterize the revealed information in terms of the shuffling parameter μ and the users' action profile $\mathbf{q}$. In what

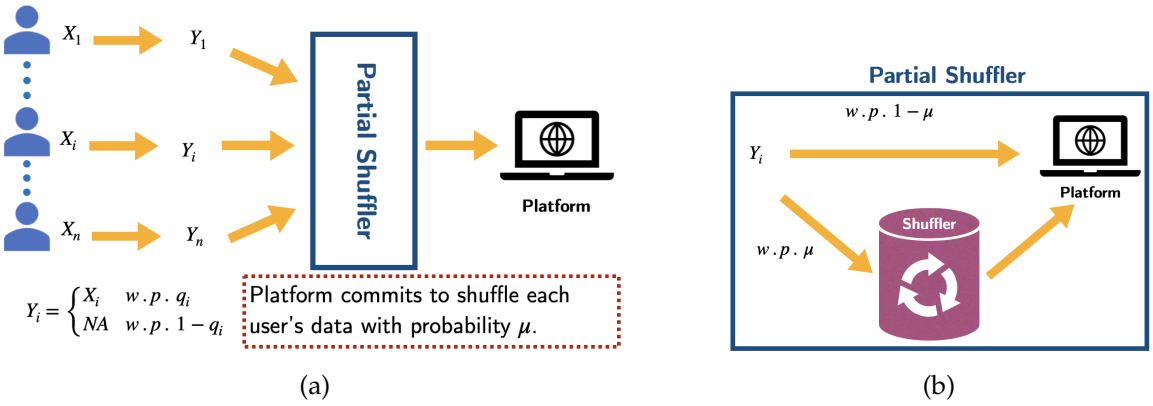

Figure 1: (a) the mask-shuffle mechanism (b) the partial shuffler.

follows, we use the following notation: for any $\mathbf{v} \in [0,1]^k$ and $j \in \{1, \cdots, k\}$, we define

$$S_j(\mathbf{v}) := \sum_{\substack{B \subseteq \{1,\cdots,k\} \\ |B|=j}} \prod_{\ell \in B} v_\ell \prod_{\ell \notin B} (1 - v_\ell). \tag{3}$$

This function is also known as the probability density function of Poisson binomial distribution, which is the number of heads after k independent coin tosses when the probability of head for coin ℓ is v_ℓ (see, e.g., Wang [1993]).

Proposition 1. *For a given $\mu \in [0,1]$ and $\mathbf{q} \in [0,1]^n$, revealed information about θ can be written as*

$$\mathcal{I}(\theta \mid \mathbf{q}, \mu) = \sum_{j=0}^{n} \frac{j}{1+j} S_j(\mathbf{q}).$$

In addition, revealed information about Z_i can be written as

$$\begin{aligned} \mathcal{I}(Z_i \mid \mathbf{q}, \mu) = (1-\mu_i) q_i \left(1 - \sum_{k=1}^{n} S_{k-1}(\mathbf{q}_{-i}) \frac{1}{1+k}\right) \\ + \sum_{k=1}^{n} \sum_{\substack{B \subseteq \mathcal{N} \\ i \in B, |B|=k}} \sum_{j=1}^{k} \sum_{r=0}^{n-k} \left(\prod_{\ell \in B} \mu_\ell\right) \left(\prod_{\ell \notin B} (1-\mu_\ell)\right) S_r(\mathbf{q}_{\mathcal{N} \setminus B}) \frac{q_i^2 S_{j-1}^2(\mathbf{q}_{B \setminus i})}{S_j(\mathbf{q}_B)} \frac{1+r}{j(1+(j+r))} \end{aligned} \tag{4}$$

where $\mathbf{q}_B := (q_\ell)_{\ell \in B}$.

This result shows that revealed information about θ does not depend on the shuffling parameter μ because irrespective of whether a user's data is shuffled or not the platform can extract the relevant information about θ in this user's data. Revealed information about Z_i, however, depends on the shuffling parameter. In fact, the first term on the right-hand side of (4) captures revealed information about Z_i when the data of user i is not shuffled, and the second term corresponds to the case that data of user i is shuffled. It is worth highlighting that, to derive the second term, we

first need to characterize the platform's belief on which one of the shuffled data belongs to user i.

We next establish that for a given desired level of revealed information about the common parameter θ, the mask-shuffle mechanism achieves the lowest possible sum of revealed information regarding private types Z_i's. Let us formalize this notion of optimality. Let

$$\mathcal{P} = \left\{ (A, B) : \ A = \mathcal{I}(\theta \mid \mathcal{M}), \ B = \sum_{i=1}^{n} \mathcal{I}(Z_i \mid \mathcal{M}) \text{ for some mechanism } \mathcal{M} \right\}$$

be the set of all pairs of revealed information about θ and revealed information about Z_i's achieved by any mechanism. Let us denote the smallest and largest possible values of A by $\underline{A}$ and $\bar{A}$, respectively. For any $A \in [\underline{A}, \bar{A}]$, the *Pareto frontier* of $\mathcal{P}$ is defined as

$$\left\{ (A, PF(A)) : \ A \in [\underline{A}, \bar{A}] \right\} \text{ where } PF(A) = \inf \left\{ B : \ (A, B) \in \mathcal{P} \right\}. \tag{5}$$

We next prove that the mask-shuffle mechanism achieves the Pareto frontier of all possible mechanisms.

Theorem 1. *For any $A \in [\underline{A}, \bar{A}]$, there exists a mask-shuffle mechanism $\mathcal{M} = (\mathbf{q}, 1)$, for some $q \in [0, 1]$, for which*

$$\mathcal{I}(\theta \mid \mathcal{M}) = A \text{ and } \sum_{i=1}^{n} \mathcal{I}(Z_i \mid \mathcal{M}) = PF(A).$$

Theorem 1 has two consequences. First, by varying the probability of sharing q from zero to one, revealed information about θ goes from zero to the highest possible level of revelation among all mechanisms. Moreover, for any given revealed information about θ in this range, the lowest possible leakage of users' private information is achieved by a mask-shuffle mechanism with a certain sharing probability q.

In closing, we should highlight that various forms of shuffling have been studied in the differential privacy literature as a technique to boost the provided privacy guarantees (see, e.g., Bittau et al. [2017] and Cheu [2021]). First, our mask-shuffle mechanism is different from simply shuffling all data points as it involves randomly masking some of the user data points and then partially and randomly shuffling them. Second, our analysis reveals the Pareto optimality of a mask-shuffle mechanism in our setting which gives it an important operational justification, unlike shuffling for the purpose of boosting privacy guarantees.

2.2 Proof of Theorem 1

Here, we present three key lemmas that together establish Theorem 1. Let us first provide the roadmap of the proof:

- We first prove that for any mechanism, the sum of the revealed information about θ and Z_i's is lower bounded by (a constant fraction of) the revealed information about $\sum_{i=1}^{n} X_i$. Intu-

itively, this holds because if a mechanism reveals too much about $\sum_{i=1}^n X_i = n\theta + \sum_{i=1}^n Z_i$, then it must be the case that it reveals information about either θ or Z_i's.

- We then establish that the revealed information about $\sum_{i=1}^n X_i$ is (a constant multiple of) the revealed information about θ. Intuitively, this holds because the conditional distribution of θ given $(X_1, \cdots, X_n)$ depends on $X_1, \cdots, X_n$ only through $\sum_{i=1}^n X_i$. Putting these two lemmas together, we establish a lower bound on the sum of the revealed information about Z_i's in terms of the revealed information about θ. This lower bound characterizes the Pareto frontier of $\mathcal{P}$, defined in (5).

- We finally prove that our mask-shuffled mechanism achieves this Pareto frontier.

We next state and prove the above results formally.

Lemma 1. *For any mechanism $\mathcal{M}$, we have*

$$\mathcal{I}(\theta \mid \mathcal{M}) + \sum_{i=1}^{n} \mathcal{I}(Z_i \mid \mathcal{M}) \geq \frac{\mathcal{I}\left(\sum_{i=1}^n X_i \mid \mathcal{M}\right)}{n^2 + n} \tag{6}$$

and the equality holds for a mask-shuffle mechanism $\mathcal{M} = (\mathbf{q}, 1)$ with any $\mathbf{q} = (q, \ldots, q)$.

Proof sketch: We briefly describe the proof idea of Lemma 1 and relegate the details to the Appendix. To show this result, we first establish a relation between the revealed information of a random variable and the square of its expectation conditioned on the mechanism $\mathcal{M}$'s output. Using this derivation, our analysis requires bounding the square of the conditional expectation of $\sum_{i=1}^n X_i = n\theta + \sum_{i=1}^n Z_i$ by the square of the conditional expectation of θ and Z_i's. To prove such a bound, we use Cauchy-Schwarz inequality and carefully tailor the weight we assign to each conditional expectation to obtain the tightest bound. We also prove that the equality case of the Cauchy-Schwarz inequality holds for our mask-shuffling mechanism by explicitly characterizing the conditional expectations in that case. ■

Lemma 1 establishes a relation among the revealed information about the underlying state θ, the users' type Z_i, and the users' data X_i. We are interested to find a relation between the revealed information about θ and Z_i's. Therefore, the next natural step is to show how the revealed information about $\sum_{i=1}^n X_i$ relates to the revealed information about θ, which is proved in our second lemma.

Lemma 2. *For any mechanism $\mathcal{M}$, we have*

$$\mathcal{I}\left(\sum_{i=1}^{n} X_i \mid \mathcal{M}\right) = (n+1)^2 \ \mathcal{I}(\theta \mid \mathcal{M}). \tag{7}$$

Proof sketch: As stated in the previous proof sketch, we know that the revealed information about θ is closely related to the conditional expectation of θ given the mechanism $\mathcal{M}$'s output. To

establish the desired result, we show that the conditional expectation of θ and $\sum_{i=1}^{n} X_i$ only differ by a constant factor. Deriving this result uses two main observations: (i) the Markov property of the mechanism: given $X_1, \cdots, X_n$, the output of the mechanism $\mathcal{M}$ is independent of θ, and (ii) the conditional distribution of θ given $(X_1, \cdots, X_n)$ only depends on $\sum_{i=1}^{n} X_i$ (the detailed proof is given in the Appendix). ■

The proof of Theorem 1 follows from plugging the relation of Lemma 1 into the bound given by Lemma 2. In particular, this proves that for any mechanism $\mathcal{M} : \mathbb{R}^n \to \mathcal{X}$, we have

$$\sum_{i=1}^{n} \mathcal{I}(Z_i \mid \mathcal{M}) \geq \frac{\mathcal{I}(\theta \mid \mathcal{M})}{n}. \tag{8}$$

Moreover, equality holds for mask-shuffle mechanism $\mathcal{M} = (\mathbf{q}, 1)$ for any $\mathbf{q} = (q, \ldots, q)$. Therefore, there is an inevitable minimum leakage of users' private information when a mechanism learns θ, and this minimum leakage increases as the mechanism reveals more about θ. Furthermore, the mask-shuffle mechanism has this minimum leakage, i.e., the mask-shuffle mechanism has the lowest possible leakage among all mechanisms that reveal equally about θ. This theorem proves the optimality of the mask-shuffle mechanism from the users' perspective.

The last remaining piece to finish the proof of Theorem 1 is to show that mask-shuffle mechanisms of the form $\mathcal{M} = (\mathbf{q}, 1)$ achieve all possible values of revealed information about θ. to see this, notice that by varying q from 0 to 1, the revealed information about θ by $\mathcal{M} = ((q, \cdots, q), 1)$, i.e., $\mathcal{I}(\theta \mid \mathbf{q}, \mu)$ goes from zero to $\frac{n}{n+1}$. The following lemma proves that no other mechanism can reveal more about θ.

Lemma 3. *The minimum (i.e., $\underline{A}$) and the maximum (i.e., $\bar{A}$) of $\mathcal{I}(\theta \mid \mathcal{M})$ over all mechanisms are 0 and $\frac{n}{n+1}$, respectively. Moreover, these bounds are achievable for a mask-shuffle mechanism $\mathcal{M} = (\mathbf{q}, 1)$ for some $q \in [0, 1]$.*

Combining Lemmas 1, 2, and 3 proves Theorem 1, establishing that the mask-shuffle mechanism achieves the Pareto frontier of revealed information about θ and revealed information about Z_i's.

2.3 The Game Between the Platform and Users

As we have seen, a mask-shuffle mechanism consists of a shuffling parameter $\mu \in [0, 1]$ and a vector of sharing probabilities $(q_1, \ldots, q_n)$. Since users own their data, we assume that they directly choose the probability with which their data will be shared with the platform, i.e., each user $i \in \mathcal{N}$ chooses q_i. We refer to $\mathbf{q}$ as the users' action profile. The shuffling parameter μ, on the other hand, is the platform's action: the platform commits to shuffle the data of each user who shares her data with probability $\mu \in [0, 1]$. The timing of the game is as follows:

1. The platform chooses her action μ, specifying the shuffling parameter.

2. Knowing the platform's shuffling parameter, all users simultaneously choose their action, specifying the probability with which they share their information with the shuffler.

The platform and the users choose their actions in an equilibrium that we introduce next.

3 Equilibrium

We use the notion of symmetric (Bayesian) Stackelberg equilibrium as our solution concept. Let us first define the user equilibrium for a given platform's action μ.

Definition 3 (user equilibrium)**.** *For a given platform's action $\mu \in [0,1]$, a user action profile $\mathbf{q} = (q, \dots, q)$ is a symmetric Bayesian Nash equilibrium if*

$$\mathcal{U}_i(\mathbf{q}, \mu) \geq \mathcal{U}_i((\mathbf{q}_{-i}, q_i = q'), \mu) \quad \text{for all } i \in \mathcal{N}, q',$$

where $\mathbf{q}_{-i} = (q_1, \dots, q_{i-1}, q_{i+1}, \dots, q_n)$.

We use the notion of symmetric equilibrium to simplify the analysis and to rule out the existence of unintuitive user equilibria. In the rest of the paper, we adopt the following assumption.

Assumption 1. *$\alpha \geq \beta$, where α and β are the weight of the revealed information about the common parameter θ and User data, respectively, in the user's utility (given in (1)).*

Assumption 1 focuses on the part of the parameter space where there is sufficient value in increasing information about the underlying common state θ. In particular, it rules out the case in which all users choose not to share their information, as we show next:

Proposition 2. *Suppose Assumption 1 holds.*

1. *For any platform's action $\mu < 1$, there exists $N(\mu)$ such that for $n \geq N(\mu)$ any symmetric user equilibrium is of the form $\mathbf{q} = (q, \dots, q)$, with $q = \frac{c}{n} + \mathcal{O}(\frac{1}{n^2})$, where c is the unique solution of*

$$\alpha \frac{1 - (c+1)e^{-c}}{c^2} = \beta(1-\mu)\left(1 - \frac{1}{c}\left(1 - \frac{1-e^{-c}}{c}\right)\right).$$

2. *For platform's action $\mu = 1$, there exists N such that for $n \geq N$, we have the following cases:*

   2.1. *If $\frac{\alpha}{\beta} \leq 2$, then any intermediary symmetric user equilibrium is of the form $\mathbf{q} = (q, \dots, q)$, where $q = \frac{\alpha}{2\beta} + \mathcal{O}\left(\frac{\log(n)}{n}\right)$. Also, $\mathbf{q} = (1, \dots, 1)$ is a user equilibrium.*

   2.2. *If $\frac{\alpha}{\beta} > 2$, then $\mathbf{q} = (1, \dots, 1)$ is the unique symmetric user equilibrium.*

To characterize the symmetric user equilibrium $(q, \cdots, q)$, we let user 1 share her data with probability q_1 and other users share their data with probability q. For $(q, \cdots, q)$ to be a symmetric user equilibrium, we must have that user 1's utility $\mathcal{U}_1(\mathbf{q}, \mu)$ as a function of q_1 is maximized by

choosing $q_1 = q$. We solve for such q by considering the first-order conditions and also checking the boundary cases. There are a few points worth mentioning. First, Assumption 1 rules out $q_i = 0$ for all $i \in \mathcal{N}$ as an equilibrium. Second, Proposition 2 characterizes the users' equilibrium action with a $1/n^2$ precision. Although characterizing the exact constant of the $1/n^2$ term is demanding, in what follows, we prove that this term only affects the lower order terms in the utility functions of the users and the platform.

We next define the Stackelberg equilibrium of the game.

Definition 4 (Stackelberg equilibrium)**.** *A pair of (q^e, μ^e) is a symmetric Stackelberg equilibrium if $\mathbf{q}^e = (q^e, \dots, q^e)$ is a symmetric user equilibrium for μ^e and*

$$\mathcal{U}_{platform}(\mathbf{q}^e, \mu^e) \geq \mathcal{U}_{platform}(\mathbf{q}', \mu'),$$

for any μ' and $\mathbf{q}'$ such that $\mathbf{q}'$ is a symmetric user equilibrium for μ'.

Theorem 2. *Suppose Assumption 1 holds. There exists a symmetric Stackelberg equilibrium (μ^e, q^e).*

Theorem 2 proves the existence of a symmetric Stackelberg equilibrium. In general, such an equilibrium may not be unique. However, in what follows, we prove the properties of the game among the users and the platform that holds for any symmetric Stackelberg equilibrium.

4 Characterization

In this section, we characterize the equilibrium and then provide some comparative statics.

Our next theorem proves that for a sufficiently large number of users if α (i.e., the weight of the revealed information about the common parameter θ in the user's utility) is small enough, then the platform's equilibrium shuffling probability is close to 1 (i.e., the platform shuffles almost all the unmasked data points). Conversely, if α is large enough, then the platform's equilibrium shuffling decision is close to 0 (i.e., the platform shuffles almost none of the unmasked data points).

Theorem 3. *Suppose $\delta \leq 1$ and Assumption 1 holds. For any $\epsilon > 0$, there exists $\underline{\alpha}$ and $\bar{\alpha}$ in $[\beta, \infty)$ and $N^e(\epsilon)$, such that for $n \geq N^e(\epsilon)$ we have:*

1. *If $\alpha \leq \underline{\alpha}$, then $\mu^e \geq 1 - \epsilon$.*
2. *If $\alpha \geq \bar{\alpha}$, then $\mu^e \leq \epsilon$.*

The proof of this theorem relies on the following steps. From Proposition 2, for any ϵ there exists $N(\epsilon)$ such that the derivation of Proposition 2 holds for $n \geq N(\epsilon)$ and $\mu \leq 1 - \epsilon$. Therefore, to find the optimal choice of μ^e for the platform, we consider two intervals $[0, 1 - \epsilon)$ and $[1 - \epsilon, 1]$ separately. In particular, we characterize the user equilibrium for any $\mu \in [0, 1 - \epsilon)$ by invoking Proposition 2, and we find the best choice of shuffling probability for the platform. We also upper

bound the platform's utility when the platform chooses $\mu \in [1-\epsilon, 1]$. Putting these two results together, we complete the proof of Theorem 3.

To understand the intuition for Theorem 3, let us consider what happens when the platform increases the shuffling parameter μ. There are two opposing forces that shape equilibrium decisions. First, for a given user action profile $\mathbf{q}$, the choice of the shuffling parameter μ does not directly change revealed information about θ (as shown in Proposition 1) but decreases revealed information about the users' data. Second, increasing the shuffling parameter μ incentivizes the users to share with a higher probability, which increases the platform's utility because it increases both revealed information about θ and about users' data. Theorem 3 establishes that for small enough α, the second force dominates and the platform's equilibrium choice is to increase the shuffling parameter very close to 1. For large enough α, on the other hand, the first force dominates and the platform's equilibrium choice is to decrease the shuffling parameter very close to 0.

We next establish our main comparative static result that establishes as α (the weight users attach to information about the underlying, common state θ) increases, they may become worse off. Recall that, holding the privacy mechanism constant, a higher α leads to greater user utility. The next theorem is therefore a paradoxical result on the response of the platform by varying the extent of privacy guarantees.

Theorem 4. *Suppose $\delta \leq 1$ and Assumption 1 holds. Then, there exists an interval (α_L, α_H) such that the user's utility at equilibrium as a function of α is decreasing over it for sufficiently large n, i.e., for any $\alpha_1 < \alpha_2$ in (α_L, α_H), there exists N such that for any $n \geq N$ the user's utility at equilibrium is larger for $\alpha = \alpha_1$ compared to $\alpha = \alpha_2$.*

We prove that this phenomenon happens when the shuffling probability μ^e at equilibrium starts to decrease from one to zero by increasing α. More precisely, as α increases, the platform takes advantage of the fact that users care more about learning the underlying common state and decreases the probability of shuffling, knowing that users will still share their data. However, the main challenge is that, at the same time, the user's gain from learning the underlying state increases. Nevertheless, we prove that the users' loss from the reduction of the shuffling parameter (and hence the increase of revealed information about their private types Z_i's) dominates their gain from learning the state θ, and hence, the total utility of users decreases.

5 Platform choice of mechanism: pivot vs. mask-shuffle mechanisms

In this section, we characterize the platform's optimal choice of mechanism and establish that platforms will in general choose mechanisms quite different from the mask-shuffle mechanism that is user-optimal, as shown above. Recall that the action of each user such as user i is her

sharing probability q_i, and

$$Y_i = \begin{cases} X_i & \text{with probability } q_i \\ \text{NA} & \text{with probability } 1 - q_i \end{cases}$$

is the input of the platform. The platform's action is a mapping from $(Y_1, \ldots, Y_n)$ to $\mathcal{X}$ for some set $\mathcal{X}$. The output of the platform's action will then be used to estimate the underlying state θ as well as the private users' data Z_i.

The mask-shuffle mechanism is one particular platform's action, but the space of all platform's actions is vast. Nevertheless, we next establish that the optimal platform's action belongs to the following class:

Definition 5 (Pivot mechanism)**.** *A pivot mechanism is defined based on a function $\sigma : \mathcal{N} \to \mathbb{R}_+$ such that: when k users share their data, the platform adds a Gaussian noise with zero mean and variance $\sigma^2(k)$ to all users who have shared.*

Intuitively, we refer to these mechanisms as "pivot mechanisms" because they increase the pivotal role of each user, as their sharing decision influences whether the platform can use the data shared by others. A special case of the pivot mechanism that is optimal from the platform's perspective is given next.

Theorem 5. *Suppose $\sigma(.)$ satisfies the following condition:*

$$\sigma^2(k-1) \geq \frac{\alpha}{\alpha - \beta} \left(\sigma^2(k) + k + 1\right) \text{ and } \sigma(n) = 0. \tag{9}$$

Then, the only symmetric user equilibrium under the pivot mechanism is $q_i = 1$ for all i. Furthermore, the platform's utility under this equilibrium is the maximum platform's utility over all possible mechanisms.

Let us first understand user behavior given such a pivot mechanism. Intuitively, inequality (9) ensures that without the user in question sharing her data there will be so much noise added to the data of other users who have shared that estimating the underlying common state, θ, becomes close to impossible for the platform. This is the sense in which the pivot mechanism makes each user pivotal: by refusing to share her data, the user makes it impossible to estimate this underlying state. If α is sufficiently large, as implied by condition (9), this is very costly for the user, and she will be convinced to sacrifice her privacy in order to allow the estimation of θ. Given this user behavior, the platform then has a strong incentive to deviate from the user-optimal mask-shuffle mechanism towards such a pivot mechanism.

To clarify the implications of this theorem, we next consider a simple form of this pivot mechanism as a corollary.

Corollary 1. *For a pivot mechanism with*

$$\sigma(k) = \begin{cases} 0 & k = n \\ \infty & k < n, \end{cases} \tag{10}$$

the unique symmetric user equilibrium is $q_i = 1$ for all i and the platform's utility is $\frac{n(n\delta+1)}{n+1}$, which is the maximum utility over all possible mechanisms.

Under the above pivot mechanism, the platform does not add any noise to users' data so long as they all share. Conversely, the platform "throws away" all users' data even if one of them does not share.

The implications for user utility are dire, however. To see this, we next characterize user welfare under the pivot mechanisms favored by the platform.

Proposition 3. *Suppose $\sigma(.)$ satisfies condition (9) so that the unique user equilibrium under the pivot mechanism is $q_i = 1$ for all i. The utility of each user is*

$$(\alpha - \beta)\frac{n}{n+1}.$$

6 Conclusion

Many platforms deploy data collected from users for a multitude of purposes. Some of these are beneficial to users, for example, when the routine sharing of their data enables platforms or others to learn more about underlying health conditions or provide better, objective recommendations to them. However, other consequences of extensive data harvesting are potentially costly for users. Some of those will directly violate their privacy and others will lead to intensive target digital ads. In the extreme, the unregulated sale of individualized data to third parties could be highly problematic for users.

When privacy costs are substantial, users may not be willing to share their data and even shy away from participation in platforms that do not provide explicit guarantees on privacy. This has motivated many platforms to introduce guidelines on how they will treat user data and offer various privacy guarantees. Despite the growing importance of this problem, we are not aware of any studies that explore how these guarantees are determined and to what extent they serve user or platform objectives.

This paper has taken a first step in this direction. We build specific a multi-stage model in which users decide whether to share their data based on the privacy-deserving mechanism choices of platforms. Our model captures several salient features of the data-related relationships between platforms and users but is still highly tractable. As a result, we are able to establish several novel results that are of both theoretical interests and provide guidance on the faultiness that exists in private data markets.

Our first result establishes that mask-shuffle mechanism, whereby the user data is fully anonymized with some probability, is Preto optimal, meaning it achieves the minimum information leakage about users' data for any given revealed information about the underlying common parameter. This also implies that it is optimal from the viewpoint of users. With mask-shuffle mechanisms, there exists a unique equilibrium in which the mechanism offered by the platform balances the utility gains from the desirable uses of data with privacy costs for users.

Our second result characterizes the (Bayesian) Stackelberg equilibrium of the game between the platform and the users. This equilibrium concept takes into account that the platform acts first by choosing (committing to) a particular mechanism for privacy preservation (and hence acts like a "Stackelberg leader' as in the game-theoretic analysis of oligopolistic markets). The label Bayesian refers to the fact that individuals make inferences about how much information will leak about the underlying state and their individual types to the user.

Third and somewhat paradoxically, we show that when the potential utility gains from data pooling increases for users (for example, because data can reveal information about underlying health conditions), users can become worse off. This result is because platforms take advantage of such changes to reduce privacy guarantees so much that user utility declines. This result should be contrasted with what would have happened if the privacy-preserving mechanism was held constant: in this case, user utility would have unambiguously increased because users would have benefited from better deployment of data. The intuition for this paradoxical result is rooted in the fact that the platform can exploit the change in user preferences to reduce privacy guarantees. Our interpretation is that this result highlights the fragility of platform-provided (self-regulated) privacy guarantees.

Finally, we explore the implications of the same forces for platform choice of data architecture. Here, we find that, even more strikingly, platforms have strong incentives to deviate from user-optimal mask-shuffle mechanisms. The reason for this finding is instructive: the platform designs a mechanism (which we refer to as a pivot mechanism) that links whether it can use other users' data to the decision of a marginal user about whether to share her own data. This makes each user pivotal: if they refuse to share their data, it becomes impossible for the platform to use the data of others to estimate the underlying common state (which is valuable for all users). With such pivotal mechanisms, the platform convinces users to sacrifice their privacy, but with significant costs to the welfare of users. This result further amplifies our conclusion that self-regulated privacy guarantees are unlikely to be sufficient for users to obtain high levels of benefit from online platform data architectures.

We view this paper as a first step in the analysis of dynamic data markets, when data can be put to a multitude of uses. Several interesting areas remain for future study. First, we assumed that the platform can fully commit to a mechanism, whereas in practice platforms can create ambiguity about how data will be used and deviate from certain promises. The analysis of these issues is more challenging, as it requires an explicit modeling of platform reputation. Second, greater heterogeneity and more diverse uses of data can be introduced into our framework. Third, users

typically participate in online platforms over many periods, and thus issues of dynamic data sharing are important in practice. These are also interesting areas for future study. Last but not least, it is important to empirically assess how users react to the prevailing privacy-preserving mechanisms and test some of the implications of this type of approach.

7 Acknowledgement

We thank participants at various seminars and conferences for comments and feedback. We gratefully acknowledge financial support from the Hewlett Foundation and the Apple Scholars in AI/ML Ph.D. fellowship.

A Proofs

This Appendix includes the omitted proofs from the text and additional results.

Properties of the revealed information measure

Here, for the sake of subsequent analysis, we first generalize the definition of revealed information, provided in Definition 1. With slight abuse of notation, we use $\mathcal{I}(.)$ in this case as well.

Definition 6. *For any real-valued random variable W and any σ-Field $\mathcal{F}$, the revealed information about W given $\mathcal{F}$ is defined as*

$$\mathcal{I}(W \mid \mathcal{F}) = \textit{Variance}(W) - \min_{\substack{\tilde{W} \text{ is} \\ \mathcal{F}-\textit{measurable}}} \mathbb{E}\left[\left(W - \tilde{W}\right)^2\right], \tag{A1}$$

where the minimization is taken over all random variables $\tilde{W}$ that are $\mathcal{F}$-measurable. In addition, for a random variable H, $\mathcal{I}(W \mid H)$ is defined as $\mathcal{I}(W \mid \sigma(H))$, where $\sigma(H)$ denotes the σ-field generated by H.

It is known [Durrett, 2019, Theorem 4.1.15] that minimum in (A1) is achieved by choosing $\tilde{W} = \mathbb{E}[W \mid \mathcal{F}]$. We next use this fact to characterize $\mathcal{I}(W \mid \mathcal{F})$.

Lemma A1. *Suppose $\mathbb{E}[W^2] < \infty$. Then,*

$$\mathcal{I}(W \mid \mathcal{F}) = \mathbb{E}\left[\mathbb{E}[W \mid \mathcal{F}]^2\right] - \mathbb{E}[W]^2.$$

Proof of Lemma A1: Given that minimum in (A1) is achieved by choosing $\tilde{W} = \mathbb{E}[W \mid \mathcal{F}]$, we should substitute $\tilde{W}$ by $\mathbb{E}[W \mid \mathcal{F}]$ in (A1). By doing so, we obtain

$$\begin{aligned}
\mathcal{I}(W \mid \mathcal{F}) &= \mathbb{E}[W^2] - \mathbb{E}[W]^2 - \mathbb{E}\left[(W - \mathbb{E}[W \mid \mathcal{F}])^2\right] \\
&= 2\mathbb{E}\left[W\, \mathbb{E}[W \mid \mathcal{F}]\right] - \mathbb{E}\left[\mathbb{E}[W \mid \mathcal{F}]^2\right] - \mathbb{E}[W]^2 \\
&= \mathbb{E}\left[\mathbb{E}[W \mid \mathcal{F}]^2\right] - \mathbb{E}[W]^2,
\end{aligned}$$

where the last equality follows from the following property of conditional expectation: for any $\mathcal{F}$-measurable random variable H, we have $\mathbb{E}[WH] = \mathbb{E}\left[\mathbb{E}[W \mid \mathcal{F}]\, H\right]$. Here we use it with $H = \mathbb{E}[W \mid \mathcal{F}]$. ■

As a consequence, the following lemma holds.

Lemma A2. *Suppose W is a zero-mean random variable with $\mathbb{E}[W^2] < \infty$. Then, for a discrete random variable H, we have*

$$\mathcal{I}(W \mid H) = \sum_{h \in supp(H)} \mathbb{P}(H = h)\mathcal{I}(W \mid H = h).$$

Proof of Lemma A2: Using Lemma A1, and since W is zero-mean, we have $\mathcal{I}(W \mid H) = \mathbb{E}\left[\mathbb{E}[W \mid \sigma(H)]^2\right]$, where the outer expectation is taken over H. Using the linearity of this expectation, we obtain the desired result. ■

Proof of Proposition 1

For θ, note that indices of data points do not matter, since all X_i's have identical distribution. Hence, shuffling does not have any effect on the estimation of θ. More formally, using Lemma A2, we have

$$\begin{aligned}\mathcal{I}(\theta \mid \mathbf{q}, \boldsymbol{\mu}) &= \sum_{j=1}^{n} \sum_{\substack{B \subseteq \{1,\cdots,n\} \\ |B|=j}} \prod_{\ell \in B} q_\ell \prod_{\ell \notin B} (1-q_\ell)\, \mathcal{I}(\theta \mid (X_k)_{k\in B}) \\ &= \sum_{j=1}^{n} \sum_{\substack{B \subseteq \{1,\cdots,n\} \\ |B|=j}} \prod_{\ell \in B} q_\ell \prod_{\ell \notin B} (1-q_\ell)\, \mathbb{E}\left[\mathbb{E}[\theta \mid (X_k)_{k\in B})]^2\right], \end{aligned} \tag{A2}$$

where the second equation follows from Lemma A1. Next, we derive $\mathbb{E}\left[\mathbb{E}[\theta \mid (X_k)_{k\in B})]^2\right]$ for any $B \subseteq \{1,\cdots,n\}$. Note that θ and $(X_k)_{k\in B}$ are jointly Gaussian, where the mean of their joint distribution is 0 and the covariance matrix of their joint distribution is given by

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 2 \end{bmatrix}. \tag{A3}$$

Hence, the distribution of θ given $(X_k)_{k\in B}$ is Gaussian, and its mean is given by

$$\mathbb{E}[\theta \mid (X_k)_{k\in B})] = [1 \cdots 1] \begin{bmatrix} 2 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 2 \end{bmatrix}^{-1} [X_k]_{k\in B}^\top. \tag{A4}$$

Using the Sherman-Morrison formula for the inverse of rank-1 perturbation of a matrix, we can write

$$\begin{bmatrix} 1+1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1+1 \end{bmatrix}^{-1} = \begin{bmatrix} 1-1/\nu & \cdots & -1/\nu \\ \vdots & \ddots & \vdots \\ -1/\nu & \cdots & 1-1/\nu \end{bmatrix}, \tag{A5}$$

with $\nu = |B| + 1$. Plugging this into (A4), yields

$$\mathbb{E}[\theta \mid (X_k)_{k\in B})] = \left(1 - \frac{|B|}{\nu}\right) [1 \cdots 1][X_k]_{k\in B}^\top = \frac{1}{|B|+1} \sum_{k\in B} X_k. \tag{A6}$$

Therefore, we have

$$\mathbb{E}\left[\mathbb{E}[\theta \mid (X_k)_{k\in B})]^2\right] = \left(\frac{1}{|B|+1}\right)^2 \mathbb{E}\left[\left(\sum_{k\in B} X_k\right)^2\right]$$
$$= \left(\frac{1}{|B|+1}\right)^2 \left(|B|^2 + |B|\right) = \frac{|B|}{|B|+1}. \tag{A7}$$

Substituting (A7) into (A2) implies

$$\mathcal{I}(\theta \mid \mathbf{q}, \boldsymbol{\mu}) = \sum_{j=1}^{n} \sum_{\substack{B\subseteq\{1,\cdots,n\} \\ |B|=j}} \prod_{\ell\in B} q_\ell \prod_{\ell\notin B} (1-q_\ell)\, \frac{j}{1+j}, \tag{A8}$$

which gives us the desired result.

Next, we focus on $\mathcal{I}(Z_i \mid \mathbf{q}, \boldsymbol{\mu})$. Using Lemma A2, we can write

$$\mathcal{I}(Z_i \mid \mathbf{q}, \boldsymbol{\mu}) = (1-\mu_i) q_i \sum_{k=1}^{n} S_{k-1}(\mathbf{q}_{-i})$$
$$\mathcal{I}(Z_i \mid \mathbf{q}, \boldsymbol{\mu}, \text{user } i \text{ data is shared and not shuffled}, k-1 \text{ other data points are shared})$$
$$+ \sum_{k=1}^{n} \sum_{\substack{B\subseteq\mathcal{N} \\ i\in B, |B|=k}} \sum_{j=1}^{k} \sum_{r=0}^{n-k} \left(\prod_{\ell\in B} \mu_\ell\right) \left(\prod_{\ell\notin B} (1-\mu_\ell)\right) S_r(\mathbf{q}_{\mathcal{N}\setminus B}) S_j(\mathbf{q}_B)$$
$$\mathcal{I}(Z_i \mid \mathbf{q}, \boldsymbol{\mu}, \text{ data of set } B \text{ is shuffled}, j \text{ data points in } B \text{ and } r \text{ data points in } \mathcal{N}\setminus B \text{ are shared}), \tag{A9}$$

where the terms of the first summation correspond to the case that the data of user i is not shuffled, and therefore the revealed information about Z_i is non-zero only if user i shares her data. Each term of the summation corresponds to having $k-1$ other data points shared (as we show next, only the number of shared data points matters in the revealed information and not their identity). The second term corresponds to the case that the data of user i is shuffled. In this case, we let B be the set of shuffled data points and we condition the events to having j data points in B and r data points in $\mathcal{N}\setminus B$ being shared. We next find the revealed information in each of these cases.

Finding $\mathcal{I}(Z_i \mid \mathbf{q}, \boldsymbol{\mu}, $ user i data is shared and not shuffled$, k-1$ other data points are shared): Using Lemma A1, we need to find the conditional expectation of Z_i. Without loss of generality, we next find the conditional expectation of Z_1 given $X_1, \ldots, X_k$. Notice that the joint distribution of $Z_1, X_1, \ldots, X_k$ is normal with covariance matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 0 \\ 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \cdots & 2 \end{bmatrix}.$$

Therefore, we have

$$\begin{aligned}\mathbb{E}[Z_1 \mid X_1,\dots,X_k] =&(1,0,\dots,0)\begin{bmatrix}2 & \cdots & 1\\ \vdots & \ddots & \vdots\\ 1 & \cdots & 2\end{bmatrix}^{-1}(X_1,\dots,X_k)^T\\ =&(1,0,\dots,0)\begin{bmatrix}1-\frac{1}{\nu_k} & \cdots & -\frac{1}{\nu_k}\\ \vdots & \ddots & \vdots\\ -\frac{1}{\nu_k} & \cdots & 1-\frac{1}{\nu_k}\end{bmatrix}^{-1}(X_1,\dots,X_k)^T\\ =&\left(1-\frac{1}{\nu_k}\right)X_1-\sum_{\ell=2}^{k}\frac{1}{\nu_k}X_\ell, \end{aligned} \tag{A10}$$

where $\nu_k = k+1$. Therefore, we have

$$\begin{aligned}&\mathcal{I}(Z_i \mid \mathbf{q},\boldsymbol{\mu}, \text{user } i \text{ data is shared and not shuffled}, k-1 \text{ other data points are shared})\\ &=\mathbb{E}\left[\left(\left(1-\frac{1}{\nu_k}\right)X_1-\sum_{\ell=2}^{k}\frac{1}{\nu_k}X_\ell\right)^2\right]=1-\frac{1}{1+k}.\end{aligned} \tag{A11}$$

Finding $\mathcal{I}(Z_i \mid \mathbf{q},\boldsymbol{\mu},$ data of set B is shuffled, j data points in B and r data points in $\mathcal{N}\backslash B$ are shared): Using Lemma A1, we need to find the conditional expectation of Z_i. We can write

$$\begin{aligned}&\mathbb{E}\left[Z_i \mid \text{ data of set } B \text{ is shuffled}, j \text{ data points in } B \text{ and } r \text{ data points in } \mathcal{N}\setminus B \text{ are shared}\right]\\ &\overset{(a)}{=}\mathbb{P}(i\in B \text{ is among those that have shared})\\ &\mathbb{E}\left[Z_i \mid \text{ data of set } B \text{ is shuffled}, j \text{ data points including } i \text{ in } B \text{ and } r \text{ data points in } \mathcal{N}\setminus B \text{ are shared}\right]\\ &\overset{(b)}{=}\mathbb{P}(i\in B \text{ is among those that have shared})\\ &\sum_{\ell=1}^{j}\frac{1}{j}\mathbb{E}\left[Z_i \mid \text{ data of set } B \text{ is shuffled}, j \text{ data points in } B \text{ and } r \text{ data points in } \mathcal{N}\setminus B \text{ are shared}, \ell\text{-th one is } i\right]\\ &\overset{(c)}{=}\mathbb{P}(i\in B \text{ is among those that have shared})\\ &\sum_{\ell=1}^{j}\frac{1}{j}\left(\left(1-\frac{1}{\nu_{j+r}}\right)\tilde{X}_\ell-\sum_{t=1,t\neq\ell}^{j+r}\frac{1}{\nu_{j+r}}\tilde{X}_t\right)\\ &\overset{(d)}{=}\mathbb{P}(i\in B \text{ is among those that have shared})\frac{1}{j}\left(\sum_{\ell=1}^{j}\left(1-\frac{j}{\nu_{j+r}}\right)\tilde{X}_\ell-\sum_{\ell=j+1}^{j+r}\frac{j}{\nu_{j+r}}\tilde{X}_\ell\right)\\ &\overset{(e)}{=}\frac{q_i S_{j-1}(\mathbf{q}_{B\backslash i})}{S_j(\mathbf{q}_B)}\frac{1}{j}\left(\sum_{\ell=1}^{j}\left(1-\frac{j}{\nu_{j+r}}\right)\tilde{X}_\ell-\sum_{\ell=j+1}^{j+r}\frac{j}{\nu_{j+r}}\tilde{X}_\ell\right),\end{aligned} \tag{A12}$$

where (a) holds because if user i does not share, then the revealed information about Z_i is zero,

(b) follows from the fact that the shuffled data points have no label and therefore i can be any of them with a uniform probability, (c) follows from a similar argument to that of (A10), (d) follows from rearranging the terms, and (e) follows from the definition of $S_k(\mathbf{q})$. Therefore, we have

$$\begin{aligned}
&\mathcal{I}(Z_i \mid \mathbf{q}, \boldsymbol{\mu}, \text{ data of set } B \text{ is shuffled}, j \text{ data points in } B \text{ and } r \text{ data points in } \mathcal{N} \setminus B \text{ are shared}) \\
&= \frac{q_i^2 S_{j-1}^2(\mathbf{q}_{B\setminus i})}{S_j^2(\mathbf{q}_B)} \frac{1}{j^2} \mathbb{E}\left[\left(\sum_{\ell=1}^{j}\left(1-\frac{j}{\nu_{j+r}}\right)\tilde{X}_\ell - \sum_{\ell=j+1}^{j+r}\frac{j}{\nu_{j+r}}\tilde{X}_\ell\right)^2\right] \\
&= \frac{q_i^2 S_{j-1}^2(\mathbf{q}_{B\setminus i})}{S_j^2(\mathbf{q}_B)} \frac{1+r}{j(1+(j+r))}. \qquad \text{(A13)}
\end{aligned}$$

By using (A11) and (A13) in (A9), we obtain

$$\begin{aligned}
\mathcal{I}(Z_i \mid \mathbf{q}, \boldsymbol{\mu}) &= (1-\mu_i) q_i \sum_{k=1}^{n} S_{k-1}(\mathbf{q}_{-i}) \left(1 - \frac{1}{1+k}\right) \\
&+ \sum_{k=1}^{n} \sum_{\substack{B\subseteq\mathcal{N} \\ i\in B, |B|=k}} \sum_{j=1}^{k}\sum_{r=0}^{n-k} \left(\prod_{\ell\in B}\mu_\ell\right)\left(\prod_{\ell\notin B}(1-\mu_\ell)\right) S_r(\mathbf{q}_{\mathcal{N}\setminus B}) S_j(\mathbf{q}_B) \frac{q_i^2 S_{j-1}^2(\mathbf{q}_{B\setminus i})}{S_j^2(\mathbf{q}_B)} \frac{1+r}{j(1+(j+r))}.
\end{aligned}$$

This completes the proof of Proposition 1. ■

Proof of Lemma 1

By using Lemma A1, for any mechanism $\mathcal{M}$, we have

$$\mathcal{I}(\sum_{i=1}^{n} X_i \mid \mathcal{M}) = \mathbb{E}\left[\left(\mathbb{E}\left[\sum_{i=1}^{n} X_i \mid \mathcal{M}\right]\right)^2\right], \quad \mathcal{I}(\theta \mid \mathcal{M}) = \mathbb{E}\left[\left(\mathbb{E}\left[\theta \mid \mathcal{M}\right]\right)^2\right],$$

and

$$\mathcal{I}(Z_i \mid \mathcal{M}) = \mathbb{E}\left[\left(\mathbb{E}\left[Z_i \mid \mathcal{M}\right]\right)^2\right] \text{ for all } i.$$

We next evaluate each term of the above expectations. We can write

$$\begin{aligned}
\mathbb{E}\left[\sum_{i=1}^{n} X_i \mid \mathcal{M}\right]^2 &= \mathbb{E}\left[n\theta + \sum_{i=1}^{n} Z_i \mid \mathcal{M}\right]^2 \\
&= \left(n\mathbb{E}\left[\theta \mid \mathcal{M}\right] + \sum_{i=1}^{n}\mathbb{E}\left[Z_i \mid \mathcal{M}\right]\right)^2 \\
&\overset{(a)}{\leq} \left(\mathbb{E}\left[\theta \mid \mathcal{M}\right]^2 + \sum_{i=1}^{n}\mathbb{E}\left[Z_i \mid \mathcal{M}\right]^2\right)(n^2 + \sum_{i=1}^{n} 1)
\end{aligned}$$

where (a) follows from Cauchy-Schwarz inequality. Taking expectation over the randomness in $\mathcal{M}$ gives us the desired bound. We next prove that equality holds when

$$\frac{1}{n}\mathbb{E}\left[\theta \mid \mathcal{M}\right] = \mathbb{E}\left[Z_i \mid \mathcal{M}\right] \text{ for all } i,$$

which is the case for $\mathcal{M} = ((q, \ldots, q), 1)$ for any q. To see this, we show that when the mechanism returns k shuffled datapoints $X_1, \cdots, X_k$, we have

$$\mathbb{E}[\theta \mid (X_\ell)_{\ell=1}^k] = \frac{1}{k+1}\sum_{\ell=1}^{k} X_\ell \text{ and} \tag{A14}$$

$$\mathbb{E}[Z_i \mid (X_\ell)_{\ell=1}^k] = \frac{1}{n(k+1)}\sum_{\ell=1}^{k} X_\ell. \tag{A15}$$

Let us prove (A14) as (A15) can be established similarly. To see why (A14) holds, note that θ and $(X_\ell)_{\ell=1}^k$ are jointly Gaussian, where the mean of their joint distribution is 0, and the covariance matrix of their joint distribution is given by

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 2 \end{bmatrix}. \tag{A16}$$

Hence, the distribution of θ given $(X_\ell)_{\ell=1}^k$ is Gaussian, and its mean is given by

$$\mathbb{E}[\theta \mid (X_\ell)_{\ell=1}^k] = [1 \cdots 1] \begin{bmatrix} 2 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 2 \end{bmatrix}^{-1} [X_1, \cdots, X_k]^\top. \tag{A17}$$

Using the Sherman-Morrison formula for the inverse of rank-1 perturbation of a matrix, we can write

$$\begin{bmatrix} 1+1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1+1 \end{bmatrix}^{-1} = \begin{bmatrix} 1-\frac{1}{k+1} & \cdots & -\frac{1}{k+1} \\ \vdots & \ddots & \vdots \\ -\frac{1}{k+1} & \cdots & 1-\frac{1}{k+1} \end{bmatrix}. \tag{A18}$$

Plugging this into (A17), yields

$$\mathbb{E}[\theta \mid (X_\ell)_{\ell=1}^k] = \left(1 - \frac{k}{k+1}\right)[1 \cdots 1][X_1, \cdots, X_k]^\top = \frac{1}{k+1}\sum_{\ell=1}^{k} X_\ell. \tag{A19}$$

This completes the proof. ■

Proof of Lemma 2

By using Lemma A1, for any mechanism $\mathcal{M}$ that has access to some random variable Y which is a function of $X_1, \ldots, X_n$, we have

$$\mathcal{I}(\theta \mid \mathcal{M}) = \mathbb{E}\left[\left(\mathbb{E}\left[\theta \mid Y\right]\right)^2\right] = \int_y f_y(y) \left(\int_\theta \theta f_{\theta|y}(\theta \mid y) d\theta\right)^2 dy$$
$$\overset{(a)}{=} \int_y \frac{1}{f_y(y)} \left(\int_\theta \theta f_{\theta,y}(\theta, y) d\theta\right)^2 dy. \tag{A20}$$

where (a) follows from Bayes' rule. Similarly, we can write

$$\mathcal{I}(\sum_{i=1}^n X_i \mid \mathcal{M}) = \int_y \frac{1}{f_y(y)} \left(\int_{x_{1:n}} \left(\sum_{i=1}^n x_i\right) f_{x_{1:n},y}(x_{1:n}, y) dx_{1:n}\right)^2 dy. \tag{A21}$$

We next compare each term of the above expressions and in particular prove that for any y,

$$\int_\theta \theta f_{\theta,y}(\theta, y) d\theta = \frac{1}{n+1} \int_{x_{1:n}} \left(\sum_{i=1}^n x_i\right) f_{x_{1:n},y}(x_{1:n}, y) d\theta$$

that together with equations (A20) and (A21), completes the proof. We can write

$$\begin{aligned}
\int_\theta \theta f_{\theta,y}(\theta, y) d\theta &\overset{(a)}{=} \int_\theta \theta \int_{x_{1:n}} f_{x_{1:n},\theta,y}(x_{1:n}, \theta, y) dx_{1:n} d\theta \\
&\overset{(b)}{=} \int_\theta \theta \int_{x_{1:n}} f_\theta(\theta) f_{x_{1:n}|\theta}(x_{1:n} \mid \theta) f_{y|x_{1:n},\theta}(y \mid x_{1:n}, \theta) dx_{1:n} d\theta \\
&\overset{(c)}{=} \int_\theta \theta \int_{x_{1:n}} f_{x_{1:n}}(x_{1:n}) f_{\theta|x_{1:n}}(\theta \mid x_{1:n}) f_{y|x_{1:n}}(y \mid x_{1:n}) dx_{1:n} d\theta \\
&\overset{(d)}{=} \int_{x_{1:n}} \left(\int_\theta \theta f_{\theta|x_{1:n}}(\theta \mid x_{1:n}) d\theta\right) f_{x_{1:n}}(x_{1:n}) f_{y|x_{1:n}}(y \mid x_{1:n}) dx_{1:n} \\
&= \int_{x_{1:n}} \mathbb{E}\left[\theta \mid x_{1:n}\right] f_{x_{1:n},y}(x_{1:n}, y) dx_{1:n} \\
&\overset{(e)}{=} \int_{x_{1:n}} \frac{\sum_{i=1}^n x_i}{n+1} f_{x_{1:n},y}(x_{1:n}, y) dx_{1:n},
\end{aligned}$$

where (a) follows from the law of total probability, (b) follows from Bayes' rule, (c) follows from the fact that the mechanism has access to $X_1, \ldots X_n$ and not θ and, therefore, conditional on $X_1, \ldots, X_n$, Y and θ are independent, and (e) follows from (A17) established in the proof of Lemma 1. It is also worth mentioning that we do a change of integration in (d). To see why we are allowed to do so, note that

$$\mathbb{E}\left[\mathbb{E}[|\theta| \mid Y]\right] \leq \mathbb{E}[|\theta|] < \infty,$$

and hence $\mathbb{E}[|\theta| \mid Y]$ is almost surely bounded, i.e.,

$$\mathbb{E}[|\theta| \mid Y = y] = \int_{\theta} \int_{x_{1:n}} |\theta| \; f_{x_{1:n},\theta|y}(x_{1:n}, \theta \mid y) dx_{1:n} d\theta < \infty \text{ a.s.}$$

Therefore,

$$\int_{\theta} \int_{x_{1:n}} |\theta| \; f_{x_{1:n},\theta,y}(x_{1:n}, \theta, y) dx_{1:n} d\theta < \infty \text{ a.s.}$$

Thus, by Fubini's theorem, we are allowed to change the order of integrals. This completes the proof. ■

Proof of Lemma 3

Among all estimators, we know that the estimator that achieves the minimum mean-squared error is the conditional expectation $\mathbb{E}[\theta \mid X_1, \cdots, X_n]$. Furthermore, the error of this estimator is equal to the error mask-shuffle mechanism $((1, \cdots, 1), 1)$, and hence the proof is complete. ■

Proof of Proposition 2

To find the symmetric the user equilibrium, for a fixed μ, suppose user 1 plays q_1 and users $2, \cdots, n$ play q, i.e., $\mathbf{q} = (q_1, q, \cdots, q)$. The symmetric user equilibrium must be such that the maximum of user 1's utility $\mathcal{U}_1(\mathbf{q}, \mu)$ as a function of q_1 is attained for $q_1 = q$. To find such q, we find the maximizer of $\mathcal{U}_1(\mathbf{q}, \mu)$ as a function of q_1 by using first order condition and then finding q such that the maximizer is $q_1 = q$. We also check the boundary cases $q = 0$ and $q = 1$ at the end.

Characterizing $\left.\frac{d\mathcal{I}(\theta \mid \mathbf{q}, \mu)}{d\, q_1}\right|_{q_1 = q}$ **:** With action profile $\mathbf{q} = (q_1, q, \cdots, q)$, we have

$$S_j(\mathbf{q}) = q_1 \binom{n-1}{j-1} q^{j-1}(1-q)^{n-j} + (1-q_1)\binom{n-1}{j} q^j (1-q)^{n-1-j}. \tag{A22}$$

Therefore, using Proposition 1, we have

$$\mathcal{I}(\theta \mid \mathbf{q}, \mu) = \sum_{j=1}^{n} \frac{j}{1+j} \left(q_1 \binom{n-1}{j-1} q^{j-1}(1-q)^{n-j} + (1-q_1)\binom{n-1}{j} q^j (1-q)^{n-1-j} \right). \tag{A23}$$

Hence, we have

$$\begin{aligned}
\frac{d\mathcal{I}(\theta \mid \mathbf{q}, \mu)}{d\, q_1} &= \sum_{j=1}^{n} \frac{j}{1+j} \binom{n-1}{j-1} q^{j-1}(1-q)^{n-j} - \sum_{j=1}^{n-1} \frac{j}{1+j} \binom{n-1}{j} q^j (1-q)^{n-1-j} \\
&= \sum_{j=0}^{n-1} \frac{j+1}{j+2} \binom{n-1}{j} q^j (1-q)^{n-1-j} - \sum_{j=0}^{n-1} \frac{j}{1+j} \binom{n-1}{j} q^j (1-q)^{n-1-j}
\end{aligned}$$

$$= 1 - \mathbb{E}_{j\sim\text{Bin}(n-1,q)}\left[\frac{1}{j+2}\right] - 1 + \mathbb{E}_{j\sim\text{Bin}(n-1,q)}\left[\frac{1}{1+j}\right]$$
$$= \mathbb{E}_{j\sim\text{Bin}(n-1,q)}\left[\frac{1}{1+j} - \frac{1}{j+2}\right]$$
$$= \mathbb{E}_{j\sim\text{Bin}(n-1,q)}\left[\frac{1}{(j+2)(j+1)}\right]. \tag{A24}$$

The above expression becomes (Chao and Strawderman [1972])

$$\frac{d\mathcal{I}(\theta \mid \mathbf{q}, \mu)}{d\, q_1} = \frac{1-(1+nq)(1-q)^n}{n(n+1)q^2}. \tag{A25}$$

Characterizing $\left.\frac{d\mathcal{I}(Z_1 \mid \mathbf{q},\mu)}{d\, q_1}\right|_{q_1=q}$: Next, we consider the revealed information of Z_1 given this action profile. By Proposition 1, we have

$$\mathcal{I}(Z_1 \mid \mathbf{q}, \mu) = A_1 + A_2, \tag{A26}$$

where

$$A_1 = (1-\mu)q_1 \sum_{k=1}^{n} S_{k-1}(\mathbf{q}_{-i})\left(1 - \frac{1}{1+k}\right),$$
$$A_2 = \sum_{k=1}^{n} \sum_{\substack{B\subseteq\mathcal{N} \\ 1\in B, |B|=k}} \sum_{j=1}^{k}\sum_{r=0}^{n-k} \mu^k(1-\mu)^{n-k} S_r(\mathbf{q}_{\mathcal{N}\setminus B}) S_j(\mathbf{q}_B) \frac{q_1^2 S_{j-1}^2(\mathbf{q}_{B\setminus 1})}{S_j^2(\mathbf{q}_B)} \frac{1+r}{j(1+(j+r))}.$$

We next evaluate A_1 and A_2. Note that $S_{k-1}(\mathbf{q}_{-1})$ is given by

$$S_{k-1}(\mathbf{q}_{-1}) = \binom{n-1}{k-1} q^{k-1}(1-q)^{n-k}.$$

Thus, by using (A22), (A28), and $\sum_{k=1}^{n} S_{k-1}(\mathbf{q}_{-1}) = 1$ we can write

$$A_1 = (1-\mu)q_1\left(1 - \sum_{k=1}^{n}\binom{n-1}{k-1} q^{k-1}(1-q)^{n-k}\frac{1}{1+k}\right). \tag{A27}$$

The above expression becomes

$$(1-\mu)q_1\left(1 - \frac{1}{nq}\left(1 - \frac{1-(1-q)^{n+1}}{(n+1)q}\right)\right)$$

whose derivative is

$$\frac{d}{dq_1}A_1 = (1-\mu)\left(1 - \frac{1}{nq}\left(1 - \frac{1-(1-q)^{n+1}}{(n+1)q}\right)\right).$$

We next evaluate derivative of A_2 with respect to q_1 at q. We first upper bound it in general, and then derive its exact form for the special case $\mu = 1$.

Note that $S_{j-1}(\mathbf{q}_{B\setminus 1})$ is given by

$$S_{j-1}(\mathbf{q}_{B\setminus 1}) = \binom{k-1}{j-1} q^{j-1}(1-q)^{k-j}. \tag{A28}$$

Thus, by using (A22), (A28), $\frac{1+r}{1+(j+r)} \leq 1$, and $\sum_{r=0}^{n-k} S_r(q_{\mathcal{N}\setminus B}) = 1$ we can write

$$\begin{aligned}
\frac{d}{dq_1} A_2 \leq & \frac{d}{dq_1} \sum_{k=1}^{n} \sum_{\substack{B\subseteq\mathcal{N} \\ 1\in B, |B|=k}} \mu^k (1-\mu)^{n-k} \sum_{j=1}^{k} \frac{q_1^2 S_{j-1}(\mathbf{q}_{B\setminus 1})^2}{j S_j(\mathbf{q}_B)} \\
= & \frac{d}{dq_1} \sum_{k=1}^{n} \sum_{\substack{B\subseteq\mathcal{N} \\ 1\in B, |B|=k}} \mu^k (1-\mu)^{n-k} \sum_{j=1}^{k} \frac{q_1^2 \left(\binom{k-1}{j-1} q^{j-1}(1-q)^{k-j}\right)^2}{j\left(q_1 \binom{k-1}{j-1} q^{j-1}(1-q)^{k-j} + (1-q_1)\binom{k-1}{j} q^j (1-q)^{k-1-j}\right)} \\
= & \frac{d}{dq_1} \sum_{k=1}^{n} \sum_{\substack{B\subseteq\mathcal{N} \\ 1\in B, |B|=k}} \mu^k (1-\mu)^{n-k} \sum_{j=1}^{k} \frac{q_1^2 \binom{k-1}{j-1} q^{j-1}(1-q)^{k-j+1}}{(jq_1(1-q) + (k-j)(1-q_1)q)}.
\end{aligned}$$

Therefore, to compute $\frac{d}{dq_1} A_2$ at $q_1 = q$, we need to characterize

$$\frac{d}{dq_1} \frac{q_1^2}{jq_1(1-q) + (k-j)(1-q_1)q} \tag{A29}$$

at q_1 which is given by

$$\begin{aligned}
& \frac{d}{dq_1} \frac{q_1^2}{jq_1(1-q) + (k-j)(1-q_1)q}\bigg|_{q_1=q} \\
& = \left(\frac{2q_1}{jq_1(1-q) + (k-j)(1-q_1)q} - \frac{(j-kq)q_1^2}{(jq_1(1-q) + (k-j)(1-q_1)q)^2}\right)\bigg|_{q_1=q} \\
& = \frac{2}{k(1-q)} - \frac{j-kq}{k^2(1-q)^2} = \frac{2k-kq-j}{k^2(1-q)^2}.
\end{aligned} \tag{A30}$$

As a consequence, we have

$$\begin{aligned}
\frac{d}{d\, q_1} A_2\bigg|_{q_1=q} \leq & \sum_{k=1}^{n} \sum_{\substack{B\subseteq\mathcal{N} \\ 1\in B, |B|=k}} \mu^k (1-\mu)^{n-k} \sum_{j=1}^{k} \binom{k-1}{j-1} q^{j-1}(1-q)^{k-j} \frac{2k-kq-j}{k^2(1-q)} \\
= & \sum_{k=1}^{n} \sum_{\substack{B\subseteq\mathcal{N} \\ 1\in B, |B|=k}} \mu^k (1-\mu)^{n-k} \frac{2k-1}{k^2}
\end{aligned}$$

$$= \sum_{k=1}^{n} \binom{n-1}{k-1} \mu^k (1-\mu)^{n-k} \frac{2k-1}{k^2}$$
$$= \frac{1}{n} \sum_{k=1}^{n} \binom{n}{k} \mu^k (1-\mu)^{n-k} \frac{2k-1}{k} = \mathcal{O}(\frac{1}{n}).$$

For the special case $\mu = 1$, we have

$$\frac{d}{d\, q_1} A_2 = \sum_{i=1}^{n} \binom{n-1}{j-1} q^{j-1} (1-q)^{n-j} \frac{2n - nq - j}{n^2(1+j)}$$
$$= \frac{2n^2 q + 2nq - 2n - 1 + (1-q)^n (2n + 1 - nq)}{n^3 (n+1) q^2}. \tag{A31}$$

Having these characterizations, we next derive the user equilibrium.

Case $\mu < 1$: In this case, we first argue qn is bounded. Let define $x := qn$. Setting the derivative of $\mathcal{U}_1(q_1, \mathbf{q}_{-1})$ evaluated at $q_1 = q$ equal to zero implies

$$\left| \alpha \left(1 - (1+x)(1 - \frac{x}{n})^n \right) - \beta(1-\mu) \left(x(x-1) + 1 - (1 - \frac{x}{n})^n \right) \right| \leq \frac{\kappa x^2}{n}, \tag{A32}$$

for some constant κ. Note that the left-hand side grows as a quadratic function with a leading coefficient $\beta(1-\mu)$ while the right-hand is a quadratic with a leading coefficient κ/n. Hence, and since $\mu < 1$, for sufficiently large n, x is bounded. Therefore, we can cast q as c/n. In this case, (A25) is equal to

$$\frac{1 - (c+1)e^{-c}}{c^2} + \mathcal{O}(\frac{1}{n}).$$

Also, derivative of A_1 is equal to

$$\frac{d}{dq_1} A_1 = (1-\mu) \left(1 - \frac{1}{c} \left(1 - \frac{1 - e^{-c}}{c} \right) \right) + \mathcal{O}(\frac{1}{n}).$$

Therefore, the derivative of $\mathcal{U}_1(q_1, \mathbf{q}_{-1})$ evaluated at $q_1 = q = \frac{c}{n}$ becomes

$$\alpha \frac{1 - (c+1)e^{-c}}{c^2} = \beta(1-\mu) \left(1 - \frac{1}{c} \left(1 - \frac{1 - e^{-c}}{c} \right) \right) + \mathcal{O}(\frac{1}{n}).$$

We next show that without the $\mathcal{O}(\frac{1}{n})$ term there exists a unique c^* that satisfies the above equation and that the derivative of the difference between the left-hand side and the right-hand side at c^* is away from zero, proving that the fixed point of the above equation is $c^* + \mathcal{O}(\frac{1}{n})$, proving that the symmetric equilibrium is given by $q = \frac{c^*}{n} + \mathcal{O}(\frac{1}{n^2})$.

Case $\mu < 1$; Proof of uniqueness of c: notice that the function

$$\alpha\frac{1-(c+1)e^{-c}}{c^2} - \beta(1-\mu)\left(1-\frac{1}{c}\left(1-\frac{1-e^{-c}}{c}\right)\right)$$

is decreasing in c. Moreover, for $c=0$, it becomes

$$\alpha\frac{1}{2} - \beta(1-\mu)\frac{1}{2} > 0,$$

where the inequality follows from Assumption 1, implying that $\alpha \geq \beta$. For $c \to \infty$, it becomes

$$-\beta(1-\mu) < 0,$$

and thus, for $\mu < 1$, for sufficiently large n, this equation has a unique solution c^*.
Proof of boundedness of the derivative: the derivative of

$$\alpha\frac{1-(c+1)e^{-c}}{c^2} - \beta(1-\mu)\left(1-\frac{1}{c}\left(1-\frac{1-e^{-c}}{c}\right)\right)$$

is

$$\alpha\frac{e^{-c}(2+c(c+2)-2e^c)}{c^3} - \beta(1-\mu)\frac{e^{-c}(2+c+(c-2)e^c)}{c^3}.$$

Evaluating the above expression at $c=c^*$ results in

$$\frac{\alpha e^{-c}}{c^3}\left((2+c(c+2)-2e^c) - (2+c+(c-2)e^c)\frac{1-(c+1)e^{-c}}{c^2-c+1-e^{-c}}\right)$$

which is strictly positive for any $c>0$. Finally, notice that c^* is strictly positive because $\alpha\frac{1}{2} - \beta(1-\mu)\frac{1}{2} > 0$ and therefore $c=0$ cannot be a solution.

Case $\mu = 1$: In this case, using (A31), we can write the first order condition as

$$\alpha\left(1-(1+nq)(1-q)^n\right) = \beta\left(2q + \frac{2q-2}{n} - \frac{1}{n^2} + (1-q)^n\frac{2n+1-nq}{n^2}\right). \tag{A33}$$

If $\alpha > 2\beta$, then one can verify that, for sufficiently large n, this equation has no solution. On the other hand, for $\alpha \leq 2\beta$, its solution is in the form of $\frac{\alpha}{2\beta} + \mathcal{O}(\log(n)/n)$.

Boundary cases $q=0$ and $q=1$: Finally, we investigate when $(0,0,\cdots,0)$ and $(1,1,\cdots,1)$ are equilibria.

- First, suppose $q=0$, and the question is when $q_1 = 0$ is the best response of user one. In this case, we have

$$\mathcal{I}(\theta \mid \mathbf{q}, \mu) = \frac{q_1}{2}, \quad \mathcal{I}(Z_1 \mid \mathbf{q}, \mu) = \frac{q_1}{2}. \tag{A34}$$

Hence, $(0, 0, \cdots, 0)$ is an equilibrium if and only if $\alpha \leq \beta$ which is ruled out by Assumption 1.

- Now, suppose suppose $q = 1$, and the question is when $q_1 = 1$ is the best response of user one. In this case, we have

$$\mathcal{I}(\theta \mid \mathbf{q}, \mu) = \frac{n-1}{n} + \frac{q_1}{n(n+1)},$$
$$\mathcal{I}(Z_1 \mid \mathbf{q}, \mu) = q_1 \left(\frac{n}{n+1} + \frac{1-(1-\mu)^n}{n} - \mu \right).$$

Thus, one could verify that $(1, 1, \cdots, 1)$ is an equilibrium if and only if

$$\frac{\alpha}{\beta} \geq 1 + (1-\mu)(n^2 - 1), \tag{A35}$$

and so, for $\mu < 1$ we can choose $N(\mu)$ such that this equilibrium is ruled out. For $\mu = 1$, however, $(1, 1, \cdots, 1)$ is an equilibrium. ■

Proof of Theorem 2

The proof simply follows from the fact that the platform's utility is a continuous function and that the set of platform's actions is the interval $[0, 1]$. ■

Proof of Theorem 3

We make use of the following two lemmas.

Lemma A3. *Suppose Assumption 1 holds. Then, for any n and any $\mu < 1$, any intermediary symmetric user equilibrium $\mathbf{q} = (q, \ldots, q)$ satisfies*

$$q \leq \frac{1}{n} \left(\sqrt{\frac{\alpha}{\beta(1-\mu)}} + 1 \right).$$

Proof of Lemma A3: Recall from the proof of Proposition 2 that any intermediary equilibrium $\mathbf{q} = (q, \cdots, q)$ satisfies

$$\alpha \frac{1-(1+nq)(1-q)^n}{n(n+1)q^2} = \beta \left((1-\mu) \left(1 - \frac{1}{nq} \left(1 - \frac{1-(1-q)^{n+1}}{(n+1)q} \right) \right) + \frac{d}{dq_1} A_2 \right), \tag{A36}$$

where A_2 is given in the proof of Proposition 2. It is straightforward to verify $\frac{d}{dq_1} A_2 \geq 0$, and hence, we have

$$\alpha \frac{1-(1+nq)(1-q)^n}{n(n+1)q^2} \geq \beta(1-\mu) \left(1 - \frac{1}{nq} \left(1 - \frac{1-(1-q)^{n+1}}{(n+1)q} \right) \right).$$

Simplifying both sides and using the bound $1 \geq 1 - (1+nq)(1-q)^n$ yields

$$\frac{\alpha}{\beta(1-\mu)} \geq n(n+1)q^2 - nq + 1 - q - (1-q)^{n+1} \geq (nq)^2 - nq.$$

If $nq \leq 1$, Lemma A3 trivially holds. Otherwise, we can lower bound the right-hand side by $(nq)^2 - 2(nq) + 1$ to obtain the desired bound. ■

We next provide an explicit expression for revealed information about the underlying common state θ and private types Z_i's under a symmetric action profile by users.

Lemma A4. *For any symmetric action profile* $\mathbf{q} = (q, \cdots, q)$*, we have*

$$\mathcal{I}(\theta \mid \mathbf{q}, \mu) \leq 1 - \frac{1}{n+1}, \tag{A37}$$

$$\mathcal{I}(Z_i \mid \mathbf{q}, \mu) \leq (1-\mu)q + \frac{1}{n(n+1)} + \frac{1-\mu}{n}. \tag{A38}$$

Furthermore, by setting $q = c/n$*, we have*

$$\mathcal{I}(\theta \mid \mathbf{q}, \mu) = 1 - \frac{1-e^{-c}}{c} + \mathcal{O}\left(\frac{1}{n}\right), \tag{A39}$$

$$\mathcal{I}(Z_i \mid \mathbf{q}, \mu) = \frac{(1-\mu)c}{n}\left(1 - \frac{e^{-c}+c-1}{c^2}\right) + \mathcal{O}(\frac{1}{n^2}). \tag{A40}$$

Proof of Lemma A4: To show (A37) and (A39), note that, for action profile $\mathbf{q} = (q, \cdots, q)$, we have

$$S_j(\mathbf{q}) = \binom{n}{j} q^j (1-q)^{n-j}. \tag{A41}$$

Thus, using Proposition 1, we have

$$\begin{aligned}
\mathcal{I}(\theta \mid \mathbf{q}, \mu) &= \sum_{j=1}^{n} \frac{j}{1+j} \binom{n}{j} q^j (1-q)^{n-j} \\
&= 1 - \sum_{j=1}^{n} \frac{1}{1+j} \binom{n}{j} q^j (1-q)^{n-j} \\
&= 1 - \mathbb{E}_{\, j \sim \text{Bin}(n,q)} \left[\frac{1}{1+j}\right] = 1 - \frac{1-(1-q)^{n+1}}{(n+1)q}
\end{aligned}$$

where the last equation follows from derivation of negative moments of binomial distribution (see Chao and Strawderman [1972] for the proof). Also, note that $\frac{1}{1+j}$ is decreasing in j, and hence, $\mathbb{E}_{\, j \sim \text{Bin}(n,q)} \left[\frac{1}{1+j}\right]$ is decreasing in q. Thus, $\mathcal{I}(\theta \mid \mathbf{q}, \mu)$ is increasing in q. Hence, setting $q = 1$ gives us (A37). Also, setting $q = c/n$ and using the fact that $(1 - c/n)^n = e^c + \mathcal{O}(1/n)$ gives us (A39).

To establish (A38) and (A40), it suffices to put $q_1 = q$ in (A26). More precisely, we have

$$\mathcal{I}(Z_1 \mid \mathbf{q}, \mu) = A_1 + A_2, \tag{A42}$$

where

$$\begin{aligned}
A_1 =& (1-\mu)q \sum_{k=1}^{n} S_{k-1}(\mathbf{q}_{-i}) \left(1 - \frac{1}{1+k}\right), \\
A_2 =& \sum_{k=1}^{n} \sum_{\substack{B \subseteq \mathcal{N} \\ 1 \in B, |B|=k}} \sum_{j=1}^{k} \sum_{r=0}^{n-k} \mu^k (1-\mu)^{n-k} S_r(\mathbf{q}_{\mathcal{N}\setminus B}) S_j(\mathbf{q}_B) \frac{q^2 S_{j-1}^2(\mathbf{q}_{B\setminus 1})}{S_j^2(\mathbf{q}_B)} \frac{1+r}{j(1+(j+r))}.
\end{aligned}$$

Using (A27), with $q_1 = q$, we can characterize A_1 as

$$(1-\mu)q \left(1 - \mathbb{E}_{\, k \sim \text{Bin}(n-1,q)} \left[\frac{1}{k+2}\right]\right) \tag{A43}$$

$$= (1-\mu)q \left(1 - \frac{1}{nq}\left(1 - \frac{1-(1-q)^{n+1}}{(n+1)q}\right)\right), \tag{A44}$$

which is bounded by $(1-\mu)q$. Also, plugging $q = c/n$, we obtain

$$A_1 = \frac{(1-\mu)c}{n}\left(1 - \frac{e^{-c}+c-1}{c^2}\right) + \mathcal{O}(\frac{1}{n^2}). \tag{A45}$$

Therefore, it remains to bound A_2:

Deriving (A38): Note that A_2/μ is the revealed information regarding Z_1, condition that data of user one has been shuffled. From the definition of revealed information, it is immediate that this term is increasing in q. Hence, we derive an upper bound for A_2 by setting $q = 1$. To do so, note that by simplifying A_2 we have:

$$A_2 = \sum_{k=1}^{n} \sum_{j=1}^{k} \sum_{r=0}^{n-k} \binom{n-1}{k-1} \binom{k-1}{j-1} \binom{n-k}{r} \mu^k (1-\mu)^{n-k} q^{j+r} (1-q)^{n-j-r} \frac{1+r}{k(1+j+r)}. \tag{A46}$$

Setting $q = 1$, only the terms with $j + r = n$ will be nonzero. This corresponds to $r = n - k$ and $j = k$. Hence, we have

$$\begin{aligned}
A_2 &\leq \sum_{k=1}^{n} \binom{n-1}{k-1} \mu^k (1-\mu)^{n-k} \frac{n-k+1}{(n+1)k} \\
&= \mu \left(\mathbb{E}_{k \sim \text{Bin}(n-1,\mu)} \left[\frac{1}{k+1}\right] - \frac{1}{n+1}\right) \\
&= \frac{1-(1-\mu)^n}{n} - \frac{\mu}{n+1}
\end{aligned} \tag{A47}$$

$$\leq \frac{1}{n} - \frac{1}{n+1} + \frac{1-\mu}{n+1}$$
$$\leq \frac{1}{n(n+1)} + \frac{1-\mu}{n},$$

which completes the proof of (A38). It is worth noting that (A47) follows from the fact that (see Chao and Strawderman [1972])

$$\mathbb{E}_{k\sim \text{Bin}(n-1,\mu)}\left[\frac{1}{k+1}\right] = \frac{1-(1-\mu)^n}{n\mu}.$$

Deriving (A40): To do so, we bound the term $\frac{1+r}{1+(j+r)} \leq 1$ in A_2 and using $\sum_{r=0}^{n-k} S_r(q_{\mathcal{N}\setminus B}) = 1$ to write

$$A_2 \leq \sum_{k=1}^{n} \sum_{\substack{B\subseteq\mathcal{N} \\ 1\in B, |B|=k}} \sum_{j=1}^{k} \mu^k (1-\mu)^{n-k} S_j(\mathbf{q}_B) \frac{q^2 S_{j-1}^2(\mathbf{q}_{B\setminus 1})}{j\, S_j^2(\mathbf{q}_B)}. \tag{A48}$$

Next, using (A41), we simplify the second term on the right hand side:

$$\begin{aligned} A_2 \leq & \sum_{k=1}^{n}\sum_{j=1}^{k} \binom{n-1}{k-1}\binom{k-1}{j-1} \mu^k (1-\mu)^{n-k} q^j (1-q)^{k-j} \frac{1}{k} \\ = & \sum_{k=1}^{n} \frac{1}{k}\binom{n-1}{k-1} \mu^k (1-\mu)^{n-k} \sum_{j=1}^{k} \binom{k-1}{j-1} q^j (1-q)^{k-j}. \end{aligned} \tag{A49}$$

Note that, we can write the inner sum as

$$\sum_{j=1}^{k} \binom{k-1}{j-1} q^j (1-q)^{k-j} = q. \tag{A50}$$

Plugging this into (A49), we obtain

$$\begin{aligned} A_2 &\leq q \sum_{k=1}^{n} \frac{1}{k}\binom{n-1}{k-1} \mu^k (1-\mu)^{n-k} \\ &= q \sum_{k=0}^{n-1} \frac{1}{k+1}\binom{n-1}{k} \mu^{k+1} (1-\mu)^{n-1-k} \\ &= q\mu\, \mathbb{E}_{k\sim \text{Bin}(n-1,\mu)}\left[\frac{1}{k+1}\right] \\ &= \frac{q\,(1-(1-\mu)^n)}{n}, \end{aligned} \tag{A51}$$

Plugging (A51) into (A42) with $q = c/n$ completes the proof of (A40). ■

We now proceed with the proof of the theorem. We choose $N^e(\epsilon) > N(\epsilon/2)$, with $N(.)$ defined in Proposition 2. Note that, by Proposition 2, for any $n \geq N(\epsilon/2)$, and for any $\mu \leq 1-\epsilon/2$, user

equilibrium is in the form of $(c+\mathcal{O}(1/n))/n$ where c satisfies

$$\alpha\frac{1-(c+1)e^{-c}}{c^2}=\beta(1-\mu)\left(1-\frac{1}{c}\left(1-\frac{1-e^{-c}}{c}\right)\right). \tag{A52}$$

We can rewrite this equation as

$$1-\mu=\frac{\alpha}{\beta}\frac{1-(c+1)e^{-c}}{c^2-c+1-e^{-c}}. \tag{A53}$$

Using Lemma A4 along with the fact that

$$\frac{1-e^{-c}}{c}$$

is Lipschitz continuous as a function of c, platform's problem can be cast as

$$\max_{\mu}\ 1-\frac{1-e^{-c}}{c}+\delta(1-\mu)c\left(1-\frac{e^{-c}+c-1}{c^2}\right)+\mathcal{O}\left(\frac{1}{n}\right) \tag{A54a}$$

$$\text{s.t.}\ \ 1-\mu=\frac{\alpha}{\beta}\frac{1-(c+1)e^{-c}}{c^2-c+1-e^{-c}} \tag{A54b}$$

$$\mu\le 1-\epsilon/2. \tag{A54c}$$

The second constraint (A54c) follows from the fact that this approximation is valid for $\mu\le 1-\epsilon/2$. We also bound the platform's utility for the case $\mu\in[1-\epsilon/2,1]$. Using Lemma A4, we can write

$$\begin{aligned}\sup_{\mu\in[1-\epsilon/2,1]}\mathcal{U}_{\text{platform}}(\mathbf{q}^e(\mu),\mu)&\le\sup_{\mu\in[1-\epsilon/2,1]}\left(1-\frac{1-\delta}{n+1}+(1-\mu)nq+1-\mu\right)\\&\le\sup_{\mu\in[1-\epsilon/2,1]}\left(1+(1-\mu)(\sqrt{\frac{\alpha}{\beta(1-\mu)}}+2)\right)\qquad\text{(A55)}\\&\le 1+\epsilon+\sqrt{\frac{\alpha\epsilon}{2\beta}},\qquad\text{(A56)}\end{aligned}$$

where (A55) follows from Lemma A3. Next, note that

$$\frac{1-(c+1)e^{-c}}{c^2-c+1-e^{-c}} \tag{A57}$$

is a deceasing function of c which varies from 1 to 0 as c goes from 0 to ∞. Hence, we could replace $1-\mu$ in (A54a) using (A54b) and replace (A54b) by the following constraint:

$$\underline{c}\le c\le\bar{c}, \tag{A58}$$

where $\underline{c}$ and $\bar{c}$ are such that

$$\left.\frac{1-(c+1)e^{-c}}{c^2-c+1-e^{-c}}\right|_{c=\underline{c}} = \frac{\beta}{\alpha}, \quad \left.\frac{1-(c+1)e^{-c}}{c^2-c+1-e^{-c}}\right|_{c=\bar{c}} = \frac{\epsilon}{2}\frac{\beta}{\alpha}. \tag{A59}$$

Using these quantities, we obtain

$$\max_c \; 1 - \frac{1-e^{-c}}{c} + \frac{\alpha\delta}{\beta}.\frac{1-(c+1)e^{-c}}{c} + \mathcal{O}\left(\frac{1}{n}\right) \tag{A60a}$$

$$\text{s.t.} \;\; \underline{c} \le c \le \bar{c}, \tag{A60b}$$

where $\underline{c}$ and $\bar{c}$ correspond to $\mu = 0$ and $\mu = 1 - \epsilon/2$, respectively. Next, note that we could choose n large enough such that the solution of (A60) and the following optimization problem in which we have removed the $\mathcal{O}\left(\frac{1}{n}\right)$ term from the objective function differ at most by $\epsilon/2$.

$$\max_c \; 1 - \frac{1-e^{-c}}{c} + \frac{\alpha\delta}{\beta}.\frac{1-(c+1)e^{-c}}{c} \tag{A61a}$$

$$\text{s.t.} \;\; \underline{c} \le c \le \bar{c} \tag{A61b}$$

Hence, it suffices to show there exists $\underline{\alpha}$ and $\bar{\alpha}$ in $[\beta, \infty)$ such that:

1. If $\alpha \le \underline{\alpha}$, then $c = \bar{c}$ which corresponds to $\mu = 1 - \epsilon/2$ being the solution of (A61). In this case, we will have $\mu^e \ge 1 - \epsilon$.
2. If $\alpha \ge \bar{\alpha}$ then $c = \underline{c}$ which corresponds to $\mu = 0$ being the solution of (A61) and the platform's utility at $c = \underline{c}$ is greater than (A56). In this case, we will have $\mu^e \le \epsilon/2$.

To show (i), notice that the derivative of (A61a) with respect to c is given by

$$\frac{e^{-c}}{c^2}\left((e^c - c - 1)(1 - \frac{\delta\alpha}{\beta}) + c^2\frac{\delta\alpha}{\beta}\right). \tag{A62}$$

If $\beta \le \alpha \le \frac{\beta}{\delta}$, then this derivative is positive, meaning that $c = \bar{c}$ is the solution of (A61). Thus, we choose $\underline{\alpha} = \frac{\beta}{\delta}$.

To show (ii), note that for α sufficiently large, we have

$$\underline{c} \ge 2, \quad \left.\frac{e^c - c - 1}{e^c - c^2 - c - 1}\right|_{c=2} \le \frac{\delta\alpha}{\beta}.$$

In this case, it is easy to verify that the derivative is negative over $[\underline{c}, \infty)$, and hence, $c = \underline{c}$ is the optimal solution of (A61). Furthermore, notice that the limit of (A61) when c goes to infinity is one. Therefore, because the platform's utility is decreasing over $[\underline{c}, \infty)$, it must be larger than one at $c = \underline{c}$. Hence, using the bound (A56), we can see that for sufficiently small ϵ and large

n, platform's utility at $c = \underline{c}$ would be greater than the maximum of platform's utility for any $\mu \in [1 - \epsilon/2, 1]$. This completes the proof. ■

Proof of Theorem 4

Recall the platform's problem given in (A60). For any $t \in [0, 1]$, we define $c(t)$ as the solution of

$$f_1(c) := \frac{1 - (c+1)e^{-c}}{c^2 - c + 1 - e^{-c}} = t. \tag{A63}$$

Using this change of variable, we can cast the platform's problem as

$$\max_t \frac{c(t) + e^{-c(t)} - 1}{c(t)} \left(1 - \frac{\delta\alpha}{\beta} t\right) + \frac{\delta\alpha}{\beta} t c(t) + \mathcal{O}\left(\frac{1}{n}\right) \tag{A64a}$$

$$\text{s.t. } \frac{\epsilon}{2} . \frac{\beta}{\alpha} \leq t \leq \frac{\beta}{\alpha}, \tag{A64b}$$

Note that (A63) is equivalent to

$$e^{c(t)} = \frac{c(t) + 1 - t}{1 + tc(t) - t - tc(t)^2}. \tag{A65}$$

Using this, we can rewrite the platform's problem (A64) as

$$\max_t g(t, \frac{\delta\alpha}{\beta}) + \mathcal{O}\left(\frac{1}{n}\right) \tag{A66a}$$

$$\text{s.t. } \frac{\epsilon}{2} \frac{\beta}{\alpha} \leq t \leq \frac{\beta}{\alpha}, \tag{A66b}$$

where

$$g(t, r) := \frac{c(t)(1-t)}{1 + c(t) - t} (1 - rt) + rtc(t) = c(t) \frac{1 - t + rtc(t)}{1 - t + c(t)} \tag{A67}$$

Also, note that, by using Lemma A4, the user's utility is given by

$$\alpha \left(1 - \frac{1 - e^{-c(t)}}{c(t)}\right) + \mathcal{O}\left(\frac{1}{n}\right) = \frac{\beta}{\delta} h(t, \frac{\delta\alpha}{\beta}) + \mathcal{O}\left(\frac{1}{n}\right), \tag{A68}$$

where

$$h(t, r) := r \frac{c(t)(1-t)}{1 - t + c(t)}. \tag{A69}$$

Claim 1. *For any $r > 1$, the function $g(., r) : [0, 1] \to \mathbb{R}$, defined in (A67), achieves its maximum over $[0, 1]$ at the unique $t^*(r)$ that satisfies*

$$\frac{\partial}{\partial t} g(t, r) \Big|_{t = t^*(r)} = 0. \tag{A70}$$

In addition, $t^*(r)$ is an increasing function of r that satisfies $\lim_{r \to 1^+} t^*(r) = 0$. Moreover, there exists

$\bar{r} > 1$ *such that* $h(t^*(r), r)$ *is decreasing in* r *over* $(1, \bar{r})$.

First, let us show how this claim gives us the result. Note that for any $\alpha > \beta/\delta$, $g(t, \frac{\delta\alpha}{\beta})$ achieves its maximum at $t^*(\frac{\delta\alpha}{\beta})$. Also, by taking $\alpha \to \beta/\delta$ from right, $t^*(\frac{\delta\alpha}{\beta}) \to 0$. Hence, we can choose $\alpha_L < \alpha_H$ and ϵ small enough such that:

1. $\frac{\beta}{\delta} < \alpha_L < \alpha_H < \bar{r}.\frac{\beta}{\delta}$ and
2. $t^*(\frac{\delta\alpha}{\beta}) \in [\frac{\epsilon}{2}.\frac{\beta}{\alpha}, \frac{\beta}{\alpha}]$ for any $\alpha \in (\alpha_L, \alpha_H)$.

Also, similar to the argument we provided in the proof of Theorem 3, we can choose ϵ small enough such that, for $\alpha \in (\alpha_L, \alpha_H)$, the platform's utility at $t = t^*(\frac{\delta\alpha}{\beta})$ be larger than the bound given by (A56) in the proof of Theorem 3. This ensures that μ^e belongs to the interval $[0, 1 - \epsilon/2]$ for $\alpha \in (\alpha_L, \alpha_H)$.

Now suppose $\alpha_1 < \alpha_2 \in (\alpha_L, \alpha_H)$. Note that, since $g(., \frac{\delta\alpha_i}{\beta})$ is increasing before its peak and decreasing after that, we have that for any small enough η, there exists $M(\eta)$, such that for any for $n > M(\eta)$ the solution of (A66) for $\alpha = \alpha_1$ and $\alpha = \alpha_2$ would be in at most η distance of $t^*(\frac{\delta\alpha_1}{\beta})$ and $t^*(\frac{\delta\alpha_2}{\beta})$, respectively.

Next, note that by the above claim, we have

$$h\left(t^*(\frac{\delta\alpha_1}{\beta}), \frac{\delta\alpha_1}{\beta}\right) > h\left(t^*(\frac{\delta\alpha_2}{\beta}), \frac{\delta\alpha_2}{\beta}\right). \tag{A71}$$

Notice that the user's utility (A68) at equilibrium for $\alpha = \alpha_i$ with $i \in \{1, 2\}$, is evaluated at the solution of (A66) which is η-close to $t^*(\frac{\delta\alpha_i}{\beta})$. Hence, by choosing η small enough and n large enough, and by using (A71), we can establish that the user's utility at equilibrium is larger with $\alpha = \alpha_1$ compared to $\alpha = \alpha_2$. This gives us the desired result. Therefore, it remains to prove the claim.

Maximum of $g(t, r)$ for $r > 1$: Note that $g(t, r)$ can be rewritten as

$$g(t, r) = g_1(c(t), r) \text{ where } g_1(c, r) = 1 - \frac{1 - e^{-c}}{c} + r\frac{1 - (c + 1)e^{-c}}{c}, \tag{A72}$$

and hence, we have

$$\frac{\partial}{\partial t}g(t, r) = \frac{\partial}{\partial c}g_1(c, r)c'(t). \tag{A73}$$

Also, note that, by inverse function theorem, $c'(t)$ is given by

$$c'(t) = \frac{1}{f_1'(c(t))}, \tag{A74}$$

and therefore, $c'(t)$ is negative over $(0, 1)$. Moreover, $\frac{\partial}{\partial c}g_1(c, r)$ is given by

$$\frac{\partial}{\partial c}g_1(c, r) = \frac{e^{-c}}{c^2}\left((e^c - c - 1)(1 - r) + c^2 r\right). \tag{A75}$$

Setting the derivative of $g_1(c,r)$ with respect to c equal to zero for $r>1$ gives

$$\frac{e^c-c-1}{c^2}=\frac{r}{r-1}. \tag{A76}$$

Notice that the left-hand side is an increasing function that goes from $1/2$ to infinity as c goes from zero to infinity. Hence, (A76) has a solution for any $r>1$ which we denote it by $c^*(r)$. Note that $f_1(c^*(r))=t^*(r)$.

The derivative $\frac{\partial}{\partial c}g_1(c,r)$ is positive for $c<c^*(r)$ which means $\frac{\partial}{\partial t}g(t,r)$ is negative for $t>t^*(r)$(because $c'(t)$ is negative). In addition, $\frac{\partial}{\partial c}g_1(c,r)$ is negative for $c>c^*(r)$ which means $\frac{\partial}{\partial t}g(t,r)$ is positive for $t\in(0,t^*(r))$. In other words, $g(t,r)$ is increasing over $(0,t^*(r))$ and decreasing over $(t^*(r),\infty)$, and thus, it achieves its maximum at $t^*(r)$.

Also, by increasing r, $r/(r-1)$ decreases which means $c^*(r)$ also decreases. But since f_1 is a decreasing function, $t^*(r)$ increases. Also, by taking $r\to 1^+$, $c^*(r)$ goes to infinity, which implies $t^*(r)\to 0^*$.

$h(t^*(r),r)$ is decreasing in r over $(1,\bar{r})$: Note that

$$\frac{d}{dr}h(t^*(r),r)=\frac{c(t^*(r))(1-t^*(r))}{1-t^*(r)+c(t^*(r))}+r\frac{d}{dr}t^*(r)\left(\frac{d}{dt}\frac{c(t)(1-t)}{1-t+c(t)}\bigg|_{t=t^*(r)}\right). \tag{A77}$$

Using the fact that

$$\frac{\partial}{\partial t}g(t,r)\bigg|_{t=t^*(r)}=0,$$

we obtain

$$\frac{d}{dt}\frac{c(t)(1-t)}{1-t+c(t)}\bigg|_{t=t^*(r)}=-\frac{r\left(c(t)+tc'^2c'(t)\right)}{(1-t)\left(1-t+rtc(t)\right)}.\frac{c(t)(1-t)}{1-t+c(t)}\bigg|_{t=t^*(r)}. \tag{A78}$$

Plugging this into (A77) implies

$$\frac{d}{dr}h(t^*(r),r)=\frac{c(t^*(r))(1-t^*(r))}{1-t^*(r)+c(t^*(r))}\left(1-\frac{r^2\left(c(t)+tc'^2c'(t)\right)}{(1-t)\left(1-t+rtc(t)\right)}\bigg|_{t=t^*(r)}.\frac{d}{dr}t^*(r)\right). \tag{A79}$$

We want to show this derivative is negative over the interval $(1,\bar{r})$. Note that for r close to one, $\frac{r^2}{1-t^*(r)}$ is close to one, and hence, if we show

$$\frac{c(t)+tc'^2c'(t)}{1-t+rtc(t)}\bigg|_{t=t^*(r)}\frac{d}{dr}t^*(r) \tag{A80}$$

is very large when r is close to one, then we are done. We next show that this term goes to infinity as r goes to one.

Recall that $t^*(r) = f_1(c^*(r))$ and thus

$$\frac{d}{dr}t^*(r) = \frac{d}{dc}f_1(c^*(r))\frac{d}{dr}c^*(r). \tag{A81}$$

Notice that (A76) implies

$$r = \kappa(c) := \frac{e^c - c - 1}{e^c - c^2 - c - 1}. \tag{A82}$$

Consequently, by inverse function theorem, we can rewrite (A81) as

$$\frac{d}{dr}t^*(r) = \frac{f_1'(c^*(r))}{\kappa'^*(r))}. \tag{A83}$$

Using this derivation along with the fact that $c'(f_1(c))) = 1/f_1'(c)$, $t = f_1(c)$, and $r = \kappa(c)$, we can rewrite (A80) as a function of c:

$$\left.\frac{cf_1'(c) + f_1(c) - f_1(c)^2}{\kappa'(c)\left(1 - f_1(c) + c\kappa(c)f_1(c)\right)}\right|_{c=c^*(r)},$$

which is equal to

$$\left.\frac{\left(e^c - 1 - c - c^2\right)^3}{c\left(e^c(c-2) + c + 2\right)\left(e^c(c^2 - c + 1) - 1\right)}\right|_{c=c^*(r)}.$$

Recall that $c^*(r)$ goes to infinity as $r \to 0^+$. Thus, this term goes to infinity as r goes to one. This completes the proof of the claim and hence Theorem 4. ■

Proof of Theorem 5

We denote user's i data after adding noise by $\tilde{X}_i$, i.e., $\tilde{X}_i = X_i + W_i$, where $W_i \sim \mathcal{N}(0, \sigma^2(k))$ if k users share their data. Suppose user one shares her data with probability q_1 and users $2, \cdots, n$ share their data with probability q. Our goal is to show the optimal choice of q_1 for user one is 1. Note that, the utility of user 1 is given by

$$\begin{aligned}
&\alpha\left(q_1\sum_{k=0}^{n-1}\binom{n-1}{k}q^k(1-q)^{n-1-k}\,\mathcal{I}(\theta \mid k+1 \text{ given users share data})\right.\\
&\quad\left.+(1-q_1)\sum_{k=0}^{n-1}\binom{n-1}{k}q^k(1-q)^{n-1-k}\,\mathcal{I}(\theta \mid k \text{ given users share data})\right)\\
&-\beta\, q_1\sum_{k=0}^{n-1}\binom{n-1}{k}q^k(1-q)^{n-1-k}\,\mathcal{I}(\theta \mid \text{data of user 1 and } k \text{ other given users is shared}).
\end{aligned}$$

Therefore, to show this term is maximized at $q_1 = 1$, we need to show the following inequality holds for any $k \in \{0, \cdots, n-1\}$:

$$\begin{aligned}\alpha\, \mathcal{I}(\theta \mid k+1 \text{ given users share data}) \geq \alpha\, \mathcal{I}(\theta \mid k \text{ given users share data}) \\ + \beta\, \mathcal{I}(\theta \mid \text{data of user 1 and } k \text{ other given users is shared}).\end{aligned}$$

To do so, without loss of generality, it suffices to show

$$\alpha\, \mathcal{I}(\theta \mid (\tilde{X}_i)_{i=1}^{k+1}) \geq \alpha\, \mathcal{I}(\theta \mid (\tilde{X}_i)_{i=1}^{k}) + \beta\, \mathcal{I}(\theta \mid (\tilde{X}_i)_{i=1}^{k+1}). \tag{A84}$$

Note that θ and $(\tilde{X}_i)_{i=1}^k$ are jointly Gaussian, where the mean of their joint distribution is 0 and the covariance matrix of their joint distribution is given by

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2+\sigma^2(k) & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 2+\sigma^2(k) \end{bmatrix}. \tag{A85}$$

Therefore, by using Sherman-Morrison formula, we establish that

$$\begin{aligned}\mathbb{E}[\theta \mid (\tilde{X}_i)_{i=1}^k] &= [1 \cdots 1] \begin{bmatrix} 2+\sigma^2(k) & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 2+\sigma^2(k) \end{bmatrix}^{-1} [X_1, \cdots, X_k]^\top \\ &= \frac{1}{k+1+\sigma^2(k)} \sum_{i=1}^k \tilde{X}_i. \end{aligned} \tag{A86}$$

As a consequence, we have

$$\mathcal{I}(\theta \mid (\tilde{X}_i)_{i=1}^k) = \mathbb{E}\left[\mathbb{E}\left[\theta \mid (\tilde{X}_i)_{i=1}^k\right]^2\right] = \frac{k}{k+1+\sigma^2(k)}. \tag{A87}$$

Next, notice that the joint distribution of $Z_1, \tilde{X}_1, \ldots, \tilde{X}_k$ is normal with covariance matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 0 \\ 1 & 2+\sigma^2(k) & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \cdots & 2+\sigma^2(k) \end{bmatrix}.$$

Similar to the previous calculations, we show

$$\mathbb{E}[Z_1 \mid (\tilde{X}_i)_{i=1}^k] = \frac{1}{1+\sigma^2(k)} \left(\frac{k+\sigma^2(k)}{k+1+\sigma^2(k)} \tilde{X}_1 - \frac{1}{k+1+\sigma^2(k)} \sum_{i=2}^k \tilde{X}_i \right). \tag{A88}$$

Hence, we have

$$\mathcal{I}(Z_1 \mid (\tilde{X}_i)_{i=1}^k) = \mathbb{E}\left[\mathbb{E}\left[Z_1 \mid (\tilde{X}_i)_{i=1}^k\right]^2\right] = \frac{k+\sigma^2(k)}{(k+1+\sigma^2(k))(1+\sigma^2(k))}. \tag{A89}$$

Plugging (A87) and (A89) into (A84), we need to show

$$\alpha\frac{k+1}{k+2+\sigma^2(k+1)} - \beta\frac{k+1+\sigma^2(k+1)}{(k+2+\sigma^2(k+1))(1+\sigma^2(k+1))} \geq \alpha\frac{k}{k+1+\sigma^2(k)}. \tag{A90}$$

Notice that we have

$$\frac{k+1}{k+2+\sigma^2(k+1)} \geq \frac{k+1+\sigma^2(k+1)}{(k+2+\sigma^2(k+1))(1+\sigma^2(k+1))}, \tag{A91}$$

and thus, to show (A90), it suffices to show

$$(\alpha-\beta)\frac{k+1}{k+2+\sigma^2(k+1)} \geq \alpha\frac{k}{k+1+\sigma^2(k)}. \tag{A92}$$

We aim to show a slightly stronger inequality by replacing k on the numerator of the left-hand side by $k+1$. In this case, $k+1$ cancels out from both sides, and we need to show

$$k+1+\sigma^2(k) \geq \frac{\alpha}{\alpha-\beta}(k+2+\sigma^2(k+1)). \tag{A93}$$

Note that, the condition on $\sigma(.)$ implies that $\sigma^2(k)$ by itself is weakly greater than the left-hand side, completing the proof. ■

Proof of Corollary 1

By using (A87) and (A89), if everyone shares their data and $\sigma(n) = 0$, then

$$\mathcal{I}(\theta \mid \text{all sharing}) = \mathcal{I}(Z_i \mid \text{all sharing}) = \frac{n}{n+1}. \tag{A94}$$

In this case, platform's utility is given by

$$(n\delta+1)\frac{n}{n+1}.$$

This is the utility corresponding to the case in the mask-shuffle mechanism that all users fully share and the platform offers no shuffling. This is the highest possible utility for the platform, but it never happens under the mask-shuffle mechanism since $(q,\mu) = ((1,\cdots,1),0)$ is never an equilibrium under the mask-shuffle mechanism. ■

Proof of Proposition 3

The proof follows from Theorem 5 and (A94). ■

References

D. Acemoglu, A. Makhdoumi, A. Malekian, and A. Ozdaglar. Too much data: Prices and inefficiencies in data markets. *American Economic Journal: Microeconomics:Micro*, 2022.

J. Anunrojwong, K. Iyer, and V. Manshadi. Information design for congested social services: Optimal need-based persuasion. *Available at SSRN 3849746*, 2021.

I. Ashlagi, M. Braverman, Y. Kanoria, and P. Shi. Clearing matching markets efficiently: informative signals and match recommendations. *Management Science*, 66(5):2163–2193, 2020.

I. Ashlagi, F. Monachou, and A. Nikzad. Optimal dynamic allocation: Simplicity through information design. In *Proceedings of the 22nd ACM Conference on Economics and Computation*, pages 101–102, 2021.

D. Bergemann and A. Bonatti. Selling cookies. *American Economic Journal: Microeconomics*, 7(3): 259–94, 2015.

D. Bergemann and A. Bonatti. Markets for information: An introduction. *Annual Review of Economics*, 11:85–107, 2019.

D. Bergemann, A. Bonatti, and T. Gan. The economics of social data. *arXiv preprint arXiv:2004.03107*, 2020.

O. Besbes and O. Mouchtaki. How big should your data really be? data-driven newsvendor and the transient of learning. *arXiv preprint arXiv:2107.02742*, 2021.

K. Bimpikis, D. Crapis, and A. Tahbaz-Salehi. Information sale and competition. *Management Science*, 65(6):2646–2664, 2019.

K. Bimpikis, I. Morgenstern, and D. Saban. Data tracking under competition. *Available at SSRN 3808228*, 2021.

A. Bittau, Ú. Erlingsson, P. Maniatis, I. Mironov, A. Raghunathan, D. Lie, M. Rudominer, U. Kode, J. Tinnes, and B. Seefeld. Prochlo: Strong privacy for analytics in the crowd. In *Proceedings of the 26th symposium on operating systems principles*, pages 441–459, 2017.

Y. Cai, C. Daskalakis, and C. Papadimitriou. Optimum statistical estimation with strategic data sources. In *Conference on Learning Theory*, pages 280–296. PMLR, 2015.

O. Candogan and K. Drakopoulos. Optimal signaling of content accuracy: Engagement vs. misinformation. *Operations Research*, 68(2):497–515, 2020.

M.-T. Chao and W. Strawderman. Negative moments of positive random variables. *Journal of the American Statistical Association*, 67(338):429–431, 1972.

Y. Chen and S. Zheng. Prior-free data acquisition for accurate statistical estimation. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, pages 659–677, 2019.

Y. Chen, N. Immorlica, B. Lucier, V. Syrgkanis, and J. Ziani. Optimal data acquisition for statistical estimation. In *Proceedings of the 2018 ACM Conference on Economics and Computation*, pages 27–44, 2018.

A. Cheu. Differential privacy in the shuffle model: A survey of separations. *arXiv preprint arXiv:2107.11839*, 2021.

R. Cummings, K. Ligett, A. Roth, Z. S. Wu, and J. Ziani. Accuracy for sale: Aggregating data with a variance constraint. In *Proceedings of the 2015 conference on innovations in theoretical computer science*, pages 317–324, 2015.

R. Cummings, H. Elzayn, V. Gkatzelis, E. Pountourakis, and J. Ziani. Optimal data acquisition with privacy-aware agents. *arXiv preprint arXiv:2209.06340*, 2022.

O. Dekel, F. Fischer, and A. D. Procaccia. Incentive compatible regression learning. *Journal of Computer and System Sciences*, 76(8):759–777, 2010.

R. Durrett. *Probability: theory and examples*, volume 49. Cambridge university press, 2019.

C. Dwork, A. Roth, et al. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407, 2014.

I. P. Fainmesser, A. Galeotti, and R. Momot. Digital privacy. *Management Science*, 2022.

A. Fallah, A. Makhdoumi, A. Malekian, and A. Ozdaglar. Optimal and differentially private data acquisition: Central and local mechanisms. *arXiv preprint arXiv:2201.03968*, 2022a.

A. Fallah, A. Makhdoumi, A. Malekian, and A. E. Ozdaglar. Bridging central and local differential privacy in data acquisition mechanisms. *Available at SSRN 4311351*, 2022b.

D. J. Foster, Z. Li, T. Lykouris, K. Sridharan, and E. Tardos. Learning in games: Robustness of fast convergence. *Advances in Neural Information Processing Systems*, 29:4734–4742, 2016.

X. Fu, N. Chen, P. Gao, and Y. Li. Privacy-preserving personalized recommender systems. *Available at SSRN 4202576*, 2022.

A. Ghosh and A. Roth. Selling privacy at auction. In *Proceedings of the 12th ACM conference on Electronic commerce*, pages 199–208, 2011.

A. Ghosh, K. Ligett, A. Roth, and G. Schoenebeck. Buying private data without verification. In *Proceedings of the fifteenth ACM conference on Economics and computation*, pages 931–948, 2014.

A. Goldfarb and C. Tucker. Online display advertising: Targeting and obtrusiveness. *Marketing Science*, 30(3):389–404, 2011.

Y. Gur, G. Macnamara, and D. Saban. On the disclosure of promotion value in platforms with learning sellers. *arXiv preprint arXiv:1911.09256*, 2019.

A. Y. Ha and S. Tong. Contracting and information sharing under supply chain competition. *Management science*, 54(4):701–715, 2008.

J. Hörner and A. Skrzypacz. Selling information. *Journal of Political Economy*, 124(6):1515–1562, 2016.

M. Hu, R. Momot, and J. Wang. Privacy management in service systems. *HEC Paris Research Paper No. MOSI-2020-1379*, 2020.

S. Ichihashi. Dynamic privacy choices. *Available at SSRN 3472151*, 2020.

N. Immorlica, Y. Kanoria, and J. Lu. When does competition and costly information acquisition lead to a deadlock? *Available at SSRN 3697165*, 2020.

S. Jagabathula, D. Mitrofanov, and G. Vulcano. Inferring consideration sets from sales transaction data. *NYU Stern School of Business*, 2020.

L. Li. Information sharing in a supply chain with horizontal competition. *Management Science*, 48 (9):1196–1212, 2002.

L. Li and H. Zhang. Confidentiality and information sharing in supply chain coordination. *Management science*, 54(8):1467–1481, 2008.

K. Ligett and A. Roth. Take it or leave it: Running a survey when privacy comes at a cost. In *International workshop on internet and network economics*, pages 378–391. Springer, 2012.

Y. Liu and Y. Chen. Learning to incentivize: Eliciting effort via output agreement. *arXiv preprint arXiv:1604.04928*, 2016.

Y. Liu and Y. Chen. Sequential peer prediction: Learning to elicit effort using posted prices. In *Thirty-First AAAI Conference on Artificial Intelligence*, 2017.

I. Lobel and W. Xiao. Optimal long-term supply contracts with asymmetric demand information. *Operations Research*, 65(5):1275–1284, 2017.

R. Meir, A. D. Procaccia, and J. S. Rosenschein. Algorithms for strategyproof classification. *Artificial Intelligence*, 186:123–156, 2012.

R. Montes, W. Sand-Zantman, and T. Valletti. The value of personal information in online markets with endogenous privacy. *Management Science*, 65(3):1342–1362, 2019.

K. Nissim, S. Vadhan, and D. Xiao. Redrawing the boundaries on purchasing data from privacy-sensitive individuals. In *Proceedings of the 5th conference on Innovations in theoretical computer science*, pages 411–422, 2014.

J. Perote and J. Perote-Pena. The impossibility of strategy-proof clustering. *Economics Bulletin*, 4 (23):1–9, 2003.

W. Shang, A. Y. Ha, and S. Tong. Information sharing in a supply chain with a common retailer. *Management Science*, 62(1):245–263, 2015.

Y. H. Wang. On the number of successes in independent trials. *Statistica Sinica*, pages 295–312, 1993.