

# Consumers' privacy data sharing between the seller and the e-commerce platform

Cheng Yan Mei Shu'e Zhong Weijun

(School of Economics and Management, Southeast University, Nanjing 210096, China)

**Abstract:** Due to the fact that consumers' privacy data sharing has multifaceted and complex effects on the e-commerce platform and its two sided agents, consumers and sellers, a game-theoretic model in a monopoly e-market is set up to study the equilibrium strategies of the three agents (the platform, the seller on it and consumers) under privacy data sharing. Equilibrium decisions show that after sharing consumers' privacy data once, the platform can collect more privacy data from consumers. Meanwhile, privacy data sharing pushes the seller to reduce the product price. Moreover, the platform will increase the transaction fee if the privacy data sharing value is high. It is also indicated that privacy data sharing always benefits consumers and the seller. However, the platform's profit decreases if the privacy data sharing value is low and the privacy data sharing level is high. Finally, an extended model considering an incomplete information game among the agents is discussed. The results show that both the platform and the seller cannot obtain a high profit from privacy data sharing. Factors including the seller's possibility to buy privacy data, the privacy data sharing value and privacy data sharing level affect the two agents' payoffs. If the platform wishes to benefit from privacy data sharing, it should increase the possibility of the seller to buy privacy data or increase the privacy data sharing value.

**Key words:** privacy data; data sharing; data sharing level; data sharing value; transaction fee

**DOI:** 10.3969/j.issn.1003-7985.2020.02.015

Consumers' privacy data is of great value to enterprises. With the help of this data, enterprises can recognize the potential consumers and send them targeted advertisement to increase sales<sup>[1-4]</sup>. In practice, enterprises' ability to collect consumers' personal data varies. In the context of e-commerce, the platform of which holds a large amount of consumer data, while sellers on the platform can only obtain a very limited amount. Take taobao.com in China as an example. Taobao.com has ob-

tained a large amount of consumer data, including consumer identity data, browsing data, transaction data, financial data, geographic location data, etc. The sellers on taobao.com can only obtain limited data related to the specific orders submitted by the consumers during the transaction. The lack of consumer data puts sellers at a disadvantage among the competition. In view of this, some e-commerce platforms share consumers' privacy data to the sellers. For example, taobao.com has launched data analysis tools. The sellers on taobao.com can pay to use these data analyzing tools to improve their marketing ability.

The impacts of privacy data sharing on the e-commerce platform, the sellers and consumers are multifaceted. For consumers, they bear more privacy risks; on the other hand, privacy data sharing enables consumers to obtain additional personalized services from sellers. For the sellers, privacy data can help them conduct accurate marketing, which is helpful to recognize the demanded consumers; on the other hand, the sellers should pay for privacy data sharing. If the sellers can obtain little value from privacy data, accepting privacy data sharing will reduce the profits of sellers. For the e-commerce platform, on the one hand, providing data sharing can increase revenue through the payment of the sellers; meanwhile, data sharing can attract more sellers to join in the platform for the value of consumers' privacy data; on the other hand, the privacy risk brought by data sharing may cause consumers to be reluctant to purchase products through the platform, thus reducing the transaction commission. In consideration of consumer privacy concerns, by studying the effects of data sharing, we can help the platform to further decide its strategy when sharing privacy data with the seller. The questions we studied specifically include: What is the impact of data sharing on the platform transaction fee setting and the seller's product price strategy? What is the impact of data sharing on the disclosure of consumers' privacy data? What is the impact of data sharing on platform profit, seller profit and consumer surplus?

Recently, researchers have studied the topic of data sharing mainly from three aspects. The first aspect is the role of personal data sharing in the competition of enterprises. For example, Casadesus-Masanell et al.<sup>[5]</sup> discussed the impact of consumer privacy concerns brought by data transaction behavior of enterprises on enterprise competition. Montes et al.<sup>[6]</sup> studied the strategy of data

**Received** 2020-01-15, **Revised** 2020-04-06.

**Biographies:** Cheng Yan (1986—), female, Ph. D. candidate; Mei Shu'e (corresponding author), female, doctor, professor, meishue@seu.edu.cn.

**Foundation item:** The National Social Science Foundation of China (No. 17BGL196).

**Citation:** Cheng Yan, Mei Shu'e, Zhong Weijun. Consumers' privacy data sharing between the seller and the e-commerce platform. [J]. Journal of Southeast University (English Edition), 2020, 36(2): 234 – 240. DOI: 10.3969/j.issn.1003-7985.2020.02.015.

dealers selling data to two competing enterprises and the impact of enterprises' purchase of consumer data on competition. The above literature studied data transaction between data supplier and data demander. These firms have no other connections. Our study focuses on data/data sharing behavior between the platform and the sellers on it. These two agents are connected by data sharing as well as product selling. Data sharing has effects on product selling. Therefore, the effects of data sharing on the agents are more complex. The second aspect is the factors that influence consumers' personal data sharing behavior<sup>[7-11]</sup>. Dinev and Hart<sup>[12]</sup> studied the impact of consumer privacy concerns on personal data disclosure and they found that the existence of privacy concerns led consumers to be reluctant to easily provide personal data on the Internet. Bansal et al.<sup>[13]</sup> explored the impact of the privacy protection mechanism on privacy data disclosure. They believed that the privacy protection mechanism strengthens consumers' trust in enterprises, which makes consumers more willing to disclose privacy data. These studies focused on the impact of consumer privacy concerns or privacy protection measures on consumer privacy data disclosure. In fact, the application of privacy data on consumers also has an effect on consumers' disclosure behaviors<sup>[14]</sup>. However, at present, there are few studies in this area. The third aspect is that much research focused on data sharing in the supply chain<sup>[15-17]</sup>. For example, Zhang et al.<sup>[18]</sup> investigated data sharing and after-sale service in the supply chain and found that data sharing did not always bring a win-win situation to the retailer and manufacturer. Most of these studies discussed the demand data and operation data of the enterprises, while we will study consumers' privacy data sharing behavior. We focused on the effects of data sharing behavior on the e-commerce platform, seller and consumers. Through constructing a game-theoretic model, we tried to explore the impacts of data sharing on the platform's transaction fee, the seller's product price setting as well as on the consumer privacy data disclosure strategy.

## 1 Model

We study the impacts of data sharing on the platform, the seller and consumers in a monopoly market through a theoretic game model. In the model, the platform helps the seller to sell its products and charge transaction fee for each transaction. Consumers buy products on the platform and meanwhile, as required, disclose personal data to the platform as a tradeoff for a personalized service. In order to help the seller operate effectively, the platform applies the data collected from consumers to the firm. We illustrate the relationship among the three agents in Fig. 1.

We assume that the platform charges the seller a transaction fee  $t$  for each sale<sup>[19]</sup>. In addition, suppose that each consumer can buy one unit product at most. There-

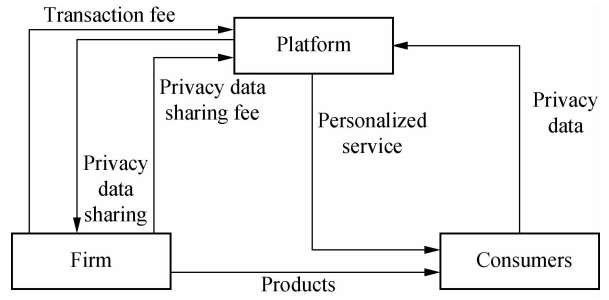


Fig. 1 Relationships among agents

fore, the platform can obtain profit  $tn$  from the transaction, where  $n$  is the number of consumers purchasing the product. On the other hand, the platform shares privacy data with the seller, which can also bring revenue. Here, we introduce parameter  $k$  referring to the privacy data sharing level, which was also described by Casadesus-Masanell et al.<sup>[5]</sup>. The privacy data sharing level determines how much data the platform will offer to share. Suppose that the quantity of data that the platform can collect from consumers is  $\sum_n y_i$ , where  $y_i$  refers to the quantity of data that each consumer discloses. Therefore, the platform will contribute  $k \sum_n y_i$  data on sharing. Given the data sharing fee  $\alpha$ , we can obtain the revenue as  $\alpha k \sum_n y_i$ . In conclusion, when sharing privacy data, the platform's profit function is

$$\varphi = \alpha k \sum_n y_i + tn \quad (1)$$

Suppose that the seller can sell products only through the platform and the cost for the sale is zero. Therefore, the profit that the seller can obtain from products is  $\sum_n (p - t)$ , where the product price  $p$  is given. Moreover, the seller can obtain benefits from consumers' privacy data. For example, with the help of the data, the seller can target potential consumers. Meanwhile, the seller can use the right keywords to describe the product so that consumers can easily search for the product. We introduce parameter  $\gamma$  to refer to the coefficient revenue from the sharing data, which can be defined as the privacy data sharing value. Furthermore, the seller has to pay for accepting privacy data, which is presented as the privacy data sharing fee  $\alpha$ . Therefore, the profit of privacy data sharing to the seller is  $(\gamma - \alpha) k \sum_n y_i$ . The profit function of the seller is

$$\pi = (\gamma - \alpha) k \sum_n y_i + \sum_n (p - t) \quad (2)$$

Consumers decide whether to buy products from two aspects. One is the utility of disclosing personal data. We assume that the valuation of data disclosing on a consumer is  $v_i$ , and the valuations of consumers in the market is uniformly distributed on  $[d^-, d^+]$ . Consumers can gain

benefits due to data disclosure. For example, the platform can offer a personalized service to them. The more consumers disclose, the more a personalized service they can obtain<sup>[5]</sup>. Therefore, given the quantity of disclosed data  $y_i$ , we assume that consumers can obtain the personalized service of  $v_i y_i$ . On the other hand, consumers suffered from disclosing due to privacy concerns. Researchers found that unauthorized use of privacy data can induce privacy concerns<sup>[14]</sup>, and data sharing increases consumers' privacy concerns<sup>[5]</sup>. Therefore, consumers' privacy concerns are  $(k+1)y_i^2$ . The other aspect of whether to buy products for a consumer is the utility of purchasing. We introduce a parameter  $\theta$  referring to the perceived value of the product. Therefore, the utility of purchasing the product is  $\theta - p$ .

To analyze the effects of data sharing, we need to consider a benchmark model where privacy data sharing is unavailable ( $k=0$ ). We construct a three-stage game, in which in the first stage, the monopolistic platform decides the transaction fee; in the second stage, the seller sets the product price; and in the final stage, consumers decide whether to buy products from the platform, and consumers who purchase decide how much privacy data they provide.

## 2 Equilibriums and Analysis

### 2.1 Equilibriums of the model

We proceed to solve the game model by backward induction and obtain the equilibrium solutions. By analyzing the equilibriums, we can obtain the effects of data sharing on the agents.

We can obtain the first-order derivative of a consumer's utility with respect to the consumer's data provision.

$$\frac{\partial u_i^D}{\partial y_i^D} = v_i(1 - 2(k+1)y_i^D) \quad (3)$$

where superscript D denotes the equilibriums for the model, in which the platform shares consumers' personal data with the seller on the platform.

Letting  $\frac{\partial u_i^D}{\partial y_i^D} = 0$ , we can obtain the equilibrium data provision of a consumer as

$$y_i^D = \frac{1}{2(k+1)} \quad (4)$$

Suppose that when the utility of consumer is positive, the consumer will purchase on the platform. There is an indifferent consumer whose utility is zero.

$$v_0 y_0^D - v_0(k+1)(y_0^D)^2 + \theta - p^D = 0 \quad (5)$$

where  $v_0$  refers to the indifferent consumer's valuation of data disclosing, and  $y_0$  refers to the indifferent consumer's data provision. Solving Eq. (5), we can obtain the indifferent data coefficient as

$$v_0^D = \frac{p^D - \theta}{y_0^D(1 - (k+1)y_0^D)} \quad (6)$$

Those consumers, whose data coefficients are higher than  $v_0$ , purchase on the platform. Therefore, we can obtain the number of consumers purchasing on the platform given data provision as

$$n^D = d^+ - \frac{p^D - \theta}{y_0^D(1 - (k+1)y_0^D)} \quad (7)$$

Analyzing Eq. (4) and Eq. (7), we can obtain the following lemmas.

**Lemma 1** Both consumers' data provision and the number of consumers purchasing on the platform decrease with the increase in a privacy data sharing level.

According to Eq. (2), we can obtain that the first-order derivative of the seller's profit  $\pi^D$  with respect to product's price is

$$\frac{\partial \pi^D}{\partial p^D} = -4(k+1) \left( (\gamma - \alpha)ky_i^D + p^D - t^D \right) + \left( d^+ - 4(k+1)(p^D - \theta) \right) \quad (8)$$

Let  $\frac{\partial \pi^D}{\partial p^D} = 0$ , and we can obtain the equilibrium price as

$$p^D = \frac{d^+}{8(k+1)} - \frac{k(\gamma - \alpha)}{4(k+1)} + \frac{t^D + \theta}{2} \quad (9)$$

**Lemma 2** The product price decreases with the decrease in privacy data sharing level and increases with the increase in transaction fee.

To maximize the profit, the platform set the transaction fee reacting to the seller's strategy and the consumer's strategy. The first-order derivative of the platform's profit  $\varphi^D$  with respect to the transaction fee is

$$\frac{\partial \varphi^D}{\partial t^D} = -4(k+1)t^D - k\alpha + \frac{d^+}{2} + k(\gamma - \alpha) + 2(k+1)\theta \quad (10)$$

Let  $\frac{\partial \varphi^D}{\partial t^D} = 0$ , and we can obtain the equilibrium transaction fee as

$$t^{D*} = \frac{d^+/2 + k(\gamma - 2\alpha)}{4(k+1)} + \frac{\theta}{2} \quad (11)$$

Similarly, as we described above, we can obtain the equilibrium transaction fee in the benchmark as

$$t^{B*} = \frac{d^+}{8} + \frac{\theta}{2} \quad (12)$$

where superscript B denotes the equilibriums for the benchmark model, in which the platform does not share consumers' personal data with the seller on the platform.

Comparing  $t^{B*}$  with the transaction fee  $t^{D*}$  in Eq. (11) when the platform is sharing privacy data, we can obtain that, if  $\gamma > d^+/2 + 2\alpha$ ,  $t^{D*} > t^{B*}$ ; otherwise, if  $\gamma \leq d^+/2$

$$+ 2\alpha, t^{D*} \leq t^{B*}.$$

**Proposition 1** Privacy data sharing encourages the platform to increase the transaction fee if the privacy data sharing value is high. Moreover, if  $\gamma > 2\alpha$ , the platform's transaction fee increases with the increase in the privacy data sharing level; otherwise, it decreases with the increase in the privacy data sharing level. In addition, the platform's transaction fee decreases with the increase in the platform's privacy data sharing fee and increases with the increase in the privacy data sharing value.

The platform would like to set a high transaction fee in order to maximize its profit. However, a high transaction fee may push the seller to opt out of the platform. If the privacy data sharing value is high enough and the seller can still profit from data sharing even though he/she has paid a high transaction fee, the seller will stay on the platform. Consequently, the platform will increase the transaction fee synchronously with the privacy data sharing level. On the other hand, if the privacy data sharing value is low, the platform has to decrease the transaction fee with the privacy data sharing level since a high transaction fee will discourage the seller to engage with it.

When sharing privacy data, the platform can increase transaction fee if privacy data sharing can help the seller gain great benefits. On the other hand, if privacy data sharing cannot bring a high revenue to the seller, the platform has to decrease the transaction fee. The platform can take two measures to increase the positive effects of privacy data sharing with the seller: 1) Set a low fee on privacy data sharing; 2) Increase the quality of privacy data.

## 2.2 Equilibriums analysis

In equilibrium, we can obtain the product price in the case of sharing privacy data as

$$p^{D*} = \frac{3d^+}{16(k+1)} - \frac{k\gamma}{8(k+1)} + \frac{3\theta}{4} \quad (13)$$

Meanwhile, in the benchmark, the seller sets the product price as

$$p^{B*} = \frac{3d^+}{16} + \frac{3\theta}{4} \quad (14)$$

**Proposition 2** Privacy data sharing causes the seller to set a lower product price no matter how much the seller has to pay for privacy data. In addition, the higher the privacy data sharing value (or privacy data sharing level) is, the lower the product price is.

Privacy data sharing, especially when the privacy data sharing value or privacy data sharing level is high, helps cut down the seller's costs on the products by accurate marketing and brings extra revenue, which can increase the seller's net profit even though product price decreases. Meanwhile, a low product price means high demand in the market.

In equilibrium, we can obtain the equilibrium demand of consumers as

$$n^D = \frac{d^+}{4} + \frac{k\gamma}{2} + (k+1)\theta \quad (15)$$

Based on the equilibrium provision and demand, we can obtain that the platform collects the sum data of  $\sum y_i^D$  from the consumers as

$$\sum y_i^D = \frac{d^+ + 2k\gamma}{8(k+1)} + \frac{\theta}{2} \quad (16)$$

The equilibrium number of potential consumers in the benchmark is

$$n^B = \frac{d^+}{4} + \theta \quad (17)$$

Based on the equilibrium provision and demand, we can obtain the platform collection of the sum data of  $\sum y_i^B$  from the consumers in the benchmark as

$$\sum y_i^B = \frac{d^+}{8} + \frac{\theta}{2} \quad (18)$$

**Proposition 3** When the platform shares privacy data, more consumers purchase on the platform. Meanwhile, the platform can collect a larger quantity of data. Moreover, the higher the privacy data sharing value or privacy data sharing level is, the more consumers the platform can attract and the more data it can collect.

Although the privacy data sharing level has increased consumers' privacy risk, it also decreases product price. Obviously, the reduction of product price brings greater positive effects on consumers. Therefore, consumers are more willing to purchase on the platform. Furthermore, even though the purchasing consumers disclose less privacy data due to privacy concerns<sup>[20-21]</sup>, the large scale of consumers increases the total quantity of data that the platform can collect.

The proposition indicates that privacy data sharing can help the platform encourage more consumers to purchase as well as collect more privacy data from them. Moreover, since the number of consumers and data collection increases with the increase in the privacy data sharing value, the platform can take measures to increase privacy data sharing value, such as preventing consumers from providing false data, regulating the sellers' transaction fraud behavior and investing to improve the data analytic capability.

In equilibrium, the profit of the platform when sharing privacy data is

$$\varphi^D = \frac{1}{2(k+1)} \left( \frac{d^+}{4} + \frac{k\gamma}{2} + (k+1)\theta \right)^2 \quad (19)$$

The profit of the platform when not sharing privacy data is

$$\varphi^B = \frac{1}{2} \left( \frac{d^+}{4} + \theta \right)^2 \quad (20)$$

Comparing  $\varphi^D$  with  $\varphi^B$ , we can obtain

$$2(k+1)\Delta\varphi = \left( \frac{\gamma}{2} + \theta \right)^2 k^2 - \left( \frac{d^+}{4} + \theta \right) \cdot \left( \frac{d^+}{4} - \theta - \gamma \right) k + \left( \frac{d^+}{4} + \theta \right)^2 \quad (21)$$

where  $\Delta\varphi = \varphi^D - \varphi^B$ .

We can obtain the results as follows:

- 1) If  $\gamma \geq d^+/8 - \frac{3}{2}\theta$ ,  $\varphi^D \geq \varphi^B$ ;
- 2) If  $\gamma < d^+/8 - \frac{3}{2}\theta$  and  $k \leq \frac{1}{2} \left( \frac{d^+}{4} + \theta \right)$ .  
 $\left( \left( \frac{d^+}{4} - \theta - \gamma \right) - \sqrt{\left( \frac{d^+}{4} + \theta \right) \left( \frac{d^+}{4} - 3\theta - 2\gamma \right)} \right) / \left( \frac{\gamma}{2} + \theta \right)^2$ ,  $\varphi^D \geq \varphi^B$ .

The profit of the firm when sharing privacy data is

$$\pi^D = \frac{n^D}{4(k+1)} \left( n^D + 2k(\gamma - \alpha) \right) \quad (22)$$

The profit of the firm when not sharing privacy data is

$$\pi^B = \left( \frac{d^+}{4} + \theta \right)^2 / 4 \quad (23)$$

The first-order derivative of the platform's profit when sharing privacy data with respect to sharing level ( $k$ ) is

$$\begin{aligned} \frac{\partial \pi^D}{\partial k} &= \frac{k}{2} \left( \frac{\partial n^D}{\partial k} \right)^2 + \\ &\quad \left( \frac{d^+/4 + \theta}{2} + \frac{k(k+2)(\gamma - \alpha)}{2(k+1)} \right) \left( \frac{\partial n^D}{\partial k} \right) + \\ &\quad \frac{(\gamma - \alpha)(d^+/4 + \theta)}{2(k+1)} \end{aligned} \quad (24)$$

Since  $\frac{\partial n^D}{\partial k} > 0$ , we can obtain that  $\frac{\partial \pi^D}{\partial k} > 0$ , which means that  $\pi^D$  increases with the increase in  $k$ . For  $k \in (0, 1]$  and  $k=0$  in the benchmark, we have  $\pi^D > \pi^B$ .

When sharing privacy data, consumer surplus is

$$CS^D = (d^+ - d^-) \cdot \left( \frac{\theta}{4} + \frac{k\gamma}{8(k+1)} - \frac{d^+}{16(k+1)} + \frac{d^-}{8(k+1)} \right) \quad (25)$$

When not sharing privacy data, consumer surplus is

$$CS^B = (d^+ - d^-) \left( \frac{\theta}{4} - \frac{d^+}{16} + \frac{d^-}{8} \right) \quad (26)$$

Comparing  $CS^D$  with  $CS^B$ , we can obtain that  $CS^D \geq CS^B$ .

**Proposition 4** Compared with the benchmark, if the platform shares privacy data to the firm, the platform earns a lower profit when the privacy data sharing value is low and the platform provides a high privacy data sharing level. In addition, both the seller's profit and consumer

surplus increase under privacy data sharing.

For the seller, privacy data sharing brings extra revenue. For the consumers, since the seller sets a low product price under privacy data sharing, their cost of obtaining the desired product decreases. Therefore, privacy data sharing benefits both the seller and the consumers. For the platform, the high privacy data sharing value can help it to set a high transaction fee, which increases the platform's profit. Under a low privacy data sharing value, the platform can increase its transaction fee only when it provides a low level of privacy data sharing, which is discussed in Proposition 1.

If the platform can collect a high quality of data and make good use of this data, privacy data sharing has a high value for the seller. Consequently, sharing privacy data is a good choice for the platform. On the other hand, if the platform cannot provide a high value of privacy data sharing, we suggest that the platform does not share privacy data. Take the two biggest e-commerce platforms, Tmall.com and JD.com, for example. Tmall.com shares while JD.com does not. We found that unlike JD.com, Tmall.com collects a large quantity of consumer data, meanwhile, it has regulations and technologies to keep this data highly valued.

### 3 Extensions

In this part, we consider the condition that the seller on the platform has a possibility to buy privacy data. Suppose that the possibility for the seller on the platform to buy privacy data is  $q$ .

The number of consumers in the market is

$$\begin{aligned} n &= q \left( \frac{d^+}{4} + k(\gamma - \alpha) + (1+k)\theta - \frac{qk(\gamma - 2\alpha)}{2} \right) + \\ &\quad (1-q) \left( \frac{d^+}{4} - \frac{qk(\gamma - 2\alpha)}{2} + (k+1)\theta \right) \end{aligned} \quad (27)$$

According to the seller's behavior, the platform sets the transaction fee as

$$t^{D*} = \frac{d^+/2 + qk(\gamma - 2\alpha)}{4(k+1)} + \frac{\theta}{2} \quad (28)$$

Furthermore, the platform can obtain an equilibrium payoff as follows:

$$\begin{aligned} \varphi^D &= \frac{q\alpha k}{2(k+1)} \left( \frac{d^+}{4} + k(\gamma - \alpha) + (1+k)\theta - \frac{qk(\gamma - 2\alpha)}{2} \right) + \\ &\quad \left( \frac{d^+}{4} + \frac{qk\gamma}{2} + (k+1)\theta \right) \left( \frac{d^+/2 + qk(\gamma - 2\alpha)}{4(k+1)} + \frac{\theta}{2} \right) \end{aligned} \quad (29)$$

Consumers' surplus is

$$CS = (d^+ - d^-) \left( -\frac{d^+}{16(k+1)} + \frac{qk\gamma}{8(k+1)} + \frac{\theta}{4} + \frac{d^-}{8(k+1)} \right) \quad (30)$$

Comparing with the equilibriums in the benchmark, we

can obtain the following results.

**Proposition 5** If the seller has a possibility to buy privacy data from the platform, privacy data sharing has the same effects on consumers' disclosing behavior, consumers' purchase behavior, the platform's transaction fee and consumers' surplus whether the seller buys privacy data or not. Moreover, privacy data sharing brings higher payoff to the platform under one of the conditions below: 1) The possibility of the seller's buying privacy data is high. 2) The possibility of the seller's buying privacy data is low and the privacy data sharing value is high. 3) The possibility of the seller's buying privacy data is low; the privacy data sharing value is low and the privacy data sharing fee is neither too high nor too low.

The proposition indicates that the seller's decision on buying privacy data influences the effects of privacy data sharing on the platform's payoff. This is because privacy data sharing can bring extra revenue to the platform if the seller buys it.

The seller decides whether to buy privacy data or not by calculating the benefits and costs of buying privacy data. If the seller does not buy privacy data, the seller sets its product price as

$$p_N^D = \frac{3d^+}{16(k+1)} + \frac{qk(\gamma-2\alpha)}{8(k+1)} + \frac{3\theta}{4} \quad (31)$$

where subscript N denotes the equilibriums for the situation that the seller does not buy privacy data from the platform.

Given the equilibrium product price, the profit of the seller is

$$\pi_N^D = \left( \frac{d^+}{16(k+1)} - \frac{qk(\gamma-2\alpha)}{8(k+1)} + \frac{\theta}{4} \right) \left( \frac{d^+}{4} + (1+k)\theta + \frac{qk\gamma}{2} \right) \quad (32)$$

In addition, if the seller buys privacy data, the seller sets the product price as

$$p_A^D = \frac{3d^+}{16(k+1)} - \frac{k(\gamma-\alpha)}{4(k+1)} + \frac{3\theta}{4} + \frac{qk(\gamma-2\alpha)}{8(k+1)} \quad (33)$$

where subscript A denotes the equilibriums for the situation that the seller buys privacy data from the platform.

Given the equilibrium product price, the profit of the seller is

$$\pi_A^D = \left( \frac{k(\gamma-\alpha)}{4(k+1)} + \frac{d^+}{16(k+1)} + \frac{\theta}{4} - \frac{qk(\gamma-2\alpha)}{8(k+1)} \right) \left( \frac{d^+}{4} + (1+k)\theta + \frac{qk\gamma}{2} \right) \quad (34)$$

Comparing with the equilibriums in the benchmark, we can obtain the following results.

**Proposition 6** The seller buys privacy data if the privacy data sharing value is lower than the privacy data sharing fee. When the seller buys privacy data, privacy data sharing makes the seller set a lower product price and the

seller can obtain a higher profit if the privacy data sharing value is high. When the seller buys privacy data, if the data service value is low ( $\gamma < 3d^+/q + 3\alpha$ ), data service makes the firm set a lower product price. Meanwhile, the seller can obtain a higher profit.

The proposition shows that if the seller does not buy privacy data, the product price may be kept lower. This indicates that privacy data sharing can decrease product price whether the seller buys privacy data or not. However, we can also see that the seller's profit cannot increase with the increase in privacy data sharing even though the seller buys privacy data. This is because an incomplete data of privacy data sharing acceptance by the seller makes the number of consumers in the market decrease.

## 4 Conclusion

The e-commerce platform profits from the transactions that the seller on it brings. Sharing privacy data with the firm, the platform can help the seller increase the possibility of getting more transactions. However, privacy data sharing increases privacy risks for the consumers, which may induce them to opt out of the market. We analyze the effects of privacy data sharing on the agents through a theoretic game model, supposing that the seller buys the privacy data once the platform provides it. The results show that: 1) In the monopoly market, privacy data sharing benefits both the seller and consumers. However, the platform's profit decreases when the privacy data sharing value is low and privacy data sharing level is high. 2) If the platform can control the data and keep the data collected at a high quality, it is a good choice for the platform to share privacy data with the seller. 3) In the extended model, the seller's decision on privacy data sharing acceptance is uncertain, and only the platform's payoff and the seller's profit are influenced by the seller's decision.

In the future, we will further discuss consumers' privacy data sharing in the context of competition. That is, how privacy data sharing works between two competing platforms or how a platform shares privacy data to competing sellers.

## References

- [1] Zhao X, Xue L. Competitive target advertising and consumer data sharing[J]. *Journal of Management Information Systems*, 2012, **29**(3): 189 – 222. DOI: 10.2753/mis0742-1222290306.
- [2] Khayati L J, Orencik C, Savas E, et al. A practical privacy-preserving targeted advertising scheme for IPTV users[J]. *International Journal of Information Security*, 2015, **15**(4): 335 – 360. DOI: 10.1007/s10207-015-0296-7.
- [3] Ha A Y, Tong S L, Zhang H T. Sharing demand information in competing supply chains with production diseconomies[J]. *Management Science*, 2011, **57**(3): 566 – 581. DOI: 10.1287/mnsc.1100.1295.
- [4] Chen J Q, Stallaert J. An economic analysis of online ad-

- vertising using behavioral targeting[J]. *MIS Quarterly*, 2014, **38**(2): 429 – 450. DOI: 10.25300/MISQ/2014/38.2.05.
- [5] Casadesus-Masanell R, Hervas-Drane A. Competing with privacy[J]. *Management Science*, 2015, **61**(1): 229 – 246. DOI: 10.1287/mnsc.2014.2023.
- [6] Montes R, Sand-Zantman W, Valletti T. The value of personal information in online markets with endogenous privacy[J]. *Management Science*, 2018, **65**(3): 1342 – 1362. DOI: 10.1287/mnsc.2017.2989.
- [7] Chen K, Rea A. Protecting personal information online: A survey of user privacy concerns and control techniques[J]. *Journal of Computer Information Systems*, 2004, **44**(4): 85 – 92. DOI: 10.1080/08874417.2004.11647599.
- [8] Chellappa R K, Shivendu S. An economic model of privacy: A property rights approach to regulatory choices for online personalization[J]. *Journal of Management Information Systems*, 2007, **24**(3): 193 – 225. DOI: 10.2753/mis0742-1222240307.
- [9] Wang T E, Duong T D, Chen C C. Intention to disclose personal information via mobile applications: A privacy calculus perspective[J]. *International Journal of Information Management*, 2016, **36**(4): 531 – 542. DOI: 10.1016/j.ijinfomgt.2016.03.003.
- [11] Korzaan M L, Boswell K T. The influence of personality traits and information privacy concerns on behavioral intentions[J]. *The Journal of Computer Information Systems*, 2008, **48**(4): 15 – 24. DOI: 10.1080/08874417.2008.11646031.
- [12] Dinev T, Hart P. Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use[J]. *e-Service Journal*, 2006, **4**(3): 25 – 59. DOI: 10.2979/esj.2006.4.3.25.
- [13] Bansal G, Zahedi F, Gefen D. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern[J]. *European Journal of Information Systems*, 2015, **24**(6): 624 – 644. DOI: 10.1057/ejis.2014.41.
- [14] Smith H J, Milberg S J, Burke S J. Information privacy: Measuring individuals' concerns about organizational practices[J]. *MIS Quarterly*, 1996, **20**(2): 167 – 196. DOI: 10.2307/249477.
- [15] Li L. Information sharing in a supply chain with horizontal competition[J]. *Management Science*, 2002, **48**(9): 1196 – 1212. DOI: 10.1287/mnsc.48.9.1196.177.
- [16] Lin X L, Wang X Q. Examining gender differences in people's information-sharing decisions on social networking sites[J]. *International Journal of Information Management*, 2020, **50**: 45 – 56. DOI: 10.1016/j.ijinfomgt.2019.05.004.
- [17] Pei Z, Yan R L. Cooperative behavior and information sharing in the e-commerce age[J]. *Industrial Marketing Management*, 2018, **76**: 12 – 22. DOI: 10.1016/j.indmarman.2018.06.013.
- [18] Zhang S G, Dan B, Zhou M S. After-sale service deployment and information sharing in a supply chain under demand uncertainty[J]. *European Journal of Operational Research*, 2019, **279**(2): 351 – 363. DOI: 10.1016/j.ejor.2019.05.014.
- [19] Chen J Q, Fan M, Li M Z. Advertising versus brokerage model for online trading platforms[J]. *MIS Quarterly*, 2016, **40**(3): 575 – 596. DOI: 10.25300/misq/2016/40.3.03.
- [20] Jiang Z J, Heng C S, Choi B C F. Research note: Privacy concerns and privacy-protective behavior in synchronous online social interactions[J]. *Information Systems Research*, 2013, **24**(3): 579 – 595. DOI: 10.1287/isre.1120.0441.
- [21] Son J-Y, Kim S S. Internet users' information privacy-protective responses: A taxonomy and a nomological model[J]. *MIS Quarterly*, 2008, **32**(3): 503 – 529. DOI: 10.2307/25148854.

## 电子商务平台与卖家间的消费者隐私数据分享行为研究

成 燕 梅姝娥 仲伟俊

(东南大学经济管理学院, 南京 210096)

**摘要:** 由于电子商务平台与平台上卖家关于消费者隐私数据的分享行为对平台、卖家和消费者带来的影响是多面及复杂的, 通过建立寡头垄断环境下的博弈模型, 研究了在平台与卖家间存在消费者隐私数据分享行为时各方的均衡策略。均衡结果显示一旦进行消费者隐私数据的分享, 平台能够收集到更多的消费者隐私数据。此外, 当消费者隐私信息分享价值较高时, 平台将会相应地提升交易佣金, 同时卖家会降低产品价格。当消费者隐私信息分享价值较低且平台数据分享程度较高时, 对消费者隐私数据的分享行为会损害平台的利益。而平台上的卖家及消费者始终可以从隐私数据分享行为中获益。最后, 对模型进行扩展, 进一步讨论了在信息不对称情形下, 即平台不确定企业是否购买隐私数据时, 平台的隐私数据分享行为对三方的影响。研究结果表明, 平台和卖家均不一定能够从隐私数据分享中获益。卖家购买隐私数据的概率、隐私数据分享的价值和分享的程度这3个因素在其中起到了重要作用。平台若想通过隐私数据分享提高收益, 只有通过提升企业购买隐私数据的可能性或提升隐私数据的分享价值来实现。

**关键词:** 隐私数据; 数据分享; 数据分享水平; 数据分享价值; 交易佣金

**中图分类号:** F272.3