Private Information Shielding Service for Overcoming Privacy Risk in Recommender System

Choong Hee Lee Junseok Hwang
lovethe2@snu.ac.kr junhwang@snu.ac.kr
Techno-Economics & Policy Program, Seoul National University, Seoul, Korea

Abstract

Recommender system has been one of the main enabler of eCommerce personalization, and there have been many researches for improving the fitness of recommendation. However, the necessity of aggregated personal information has pointed out the privacy risk of recommender system. In this paper, we provide basic framework for analyzing the behavior of private information sharing in recommender system, and based on the analysis emphasize the importance of securing trust in eCommerce system. Finally, we suggest the PRINSS-PRivate INformation Shielding Service for enhancing current recommender system by reducing privacy risk with minimizing the deterioration of recommendation.

1. Introduction

It has been only 25 years when we started to experience varieties of web applications and World Wide Web systems, but there already existed more than 7,700 terabytes of information on the web and more than 5 billion people got connected to this enormous amount of information by year 2000[1]. Increasing rate of these enormous amounts of information on the web has accelerated with the passage of time and the importance of finding suitable information for each individual has increased. By this reason, people have wanted systems, which can provide valuable information for each individual, and the representative system to satisfy these requests is recommender system. Recommender system is defined as the personalized information providing system through explicit or implicit data collection about all the system users. The developers of the first recommender system, Tapestry, coined the phrase “collaborative filtering” and several others have adopted it[2][3], but now it is considered as one of the technical approaches to operate the recommender system. Collaborative filtering, which is one of the most popular algorithm to embody the recommender system, is operated by looking for patterns of agreement among the ratings of groups of people[4]. The rating includes both users’ explicit indication of preferences about items and implicit indication, such as purchases or click-throughs. The collaborative filtering functions to predict and inform the user about specific items, which are more probable to prefer by analyzing the patterns of the similar rating groups. Recommender system in a broad sense includes the systems which are operated by cross-sell list or the recommendation from product experts. However, in this paper, we will mainly focus on the situation of eCommerce, using the automatic recommender system. It is because

of the incremental necessity in automatic recommender system with the demand expansion for real-time personalized online services. In reality, technology development such as data center and information retrieval is widening the adoption of autonomous recommender system in the applications of eCommerce services.

2. Benefits of the Recommender System in ECommerce

As one of the factors to raise the sales in eCommerce, Group Lens Research Project team presented the benefits of the recommender system as followings. [5]

- Converting Browsers into Buyers
- Increasing Cross-sell
- Building Loyalty

Above benefits are from the viewpoint of sellers, and the benefits of the customers from recommender system are like followings.

- Decreasing the uncertainty of outcome with product purchasing
- Decreasing the searching cost for the product

These benefits for the user contribute to the increment of expected utility from buying the product, and it can cause the growth of purchasing amount as a result when the product price is kept in similar level. If people have risk-averse utility function, the changes of the customer benefit from recommender system existence can be expressed like below.

☐ When there doesn't exist a recommender system(RS),

- Uncertain outcome of the product before purchasing :X
- Expected utility of product purchasing: $E(u(X))$
- Utility decrement due to the product searching effort :U_C
- Expected consumer surplus(CS) of transaction : $E(u(X)) - U_C - P$
- Buying condition without RS: $CS \geq 0$ - (1)

☐ Changes when there exist a recommender system(RS),

- Uncertain outcome of the product before purchasing: X_1
- Reduction of uncertainty in product outcome: $E(u(X_1)) > E(u(X))$
- Reduction of the utility decrement due to searching: $U_{C1} < U_C$

- Increment of expected *CS* of transaction: $\triangle CS = CS_1 - CS\ (>0)$
- Changed Buying condition with RS: $CS \geq -\triangle CS$ - (2)

As shown in above numerical expressions, condition (1) is included in condition (2). Accordingly, it is clear that the number of the customers, who transact the products, increase with the support of recommender system. Even when the product price rises by △P because of RS deployment cost, the demands for the product can increase if the product uncertainty and searching cost decreases enough. However, the efficient operation of RS needs to aggregate private information. Therefore, there exists trade-off relationship between the fitness of recommendation and the risk of private information outflow[6].

3. Fitness of Recommendation vs. Protection of Personal Information

In order to produce personalized recommendation, the recommender system requires private information of recommender system constituents. Recommender system, following its algorithm, predicts and provides the information about the most appropriate item for the user, based on personal information supplied by users. Algorithms of recommender system can be categorized by the item-item algorithm and the user-user algorithm[7]. The item-item algorithm computes and utilizes the similarities among the items, and user-user algorithm among the users. In order to calculate similarities, various kinds of personal information are required, and the correctness of recommender system depends on how much information has been provided. For generating more suitable recommendation, larger amount of personal information is required. Accordingly, performance of recommender system shows positive correlation with privacy risk in general cases. In addition to this, the fact, which the major constraints in the promotion of eCommerce adoption is customers' concerning about private information out-flow, makes the privacy problem of recommender system more serious[8]. With such a reason, researchers have developed several solutions to keep the efficiency of the recommender system, at the same time, protecting the personal information of the users[9]. However, each solution has its own shortcoming and it is like followings.

□ Pseudonymous Profiles

For protecting personal information of system users, an anonymous identity is provided. Privacy risk can be reduced because aggregated pseudonymous profiles are hard to match with real identities. However, during the process which should be related with real identity like payment and delivery, the risk of revealing real owner of anonymous profile exists. In this case, it is very hard to protect both user's privacy and the input data for recommendation system because the clear separation between real identity and anonymous profile will prohibit storing all the information connected to

real identity. In eCommerce, the process requiring real identity is unavoidable, and the information related with this process takes large portion of recommender system's input data. On this reason, this kind of solution has limitation in being implemented to current eCommerce system.

☐ Client-Side Profiles

Another option for reducing the privacy concern is to store personal information on the end-user devices. Privacy can be protected by forbidding recommender system operator to aggregate personal profiles. For aggregating users' personal information without privacy concerning, architecture in which participants compute a "public aggregate" of their data to share with members of their community is proposed by Canny[10]. The problem of this solution is that the aggregation of personal information of all required users is hard to be conducted. This is why the organization of personal information sharer is hard to have the same members with the organization required for recommendation. Accordingly, the amount of input data for recommender algorithm is likely to lessen, and this means that certain amount of drop in recommendation fitness is unavoidable. Additionally, this solution increases the privacy risk by viruses or other malicious programs which targets personal devices, and needs operating overhead comes from distributed ad-hoc end-user devices.

☐ Task-based Personalization.

The temporary information, which is obtained by activated session or task, is utilized for the input of recommender system to produce real time personalized recommendation. This solution has clear limitation in the services which need permanent information or history of purchasing.

☐ Putting users in Control

This is the method to build a system which needs to receive the approval of owner of personal information for the application of all source of personal information. It can be the most basic and independent approach to the problems which are related to privacy, but a regulatory and technological support is required for securing the usage of personal information in only authorized areas. However, recommender system operator has incentive to utilize shared personal information to unauthorized purposes because it can enhance the performance comparing to competing systems. This observable incentive makes the decision of personal information sharing difficult, and the decrement of shared information increases the incentive(value of unauthorized utilization) of RS operator's violating individual privacy policy at the same time. Moreover, monitoring the usage of once supplied data is almost impossible, and this also increases the privacy concern from personal information sharing. According to formerly described reasons, it is hard to guarantee users' control about personal information in reality, and users are likely to hide their personal information.

In the area of eCommerce, the P3P(Platform for Privacy Preference) is the representative technology, which alleviates consumer concerns about privacy while maintaining the possibility of efficient recommender system[11]. The P3P solution has great advantages for recommenders by providing a persistent identifier. On the other hand, P3P has potentialities of generating critical damage to recommender system through enlarging personal information hiding. By reason of this, the biggest uncertainty of P3P to the recommender system is not to share the personal information or provides false information because of privacy concern. Of course, in the case when the personal information is not supplied, the consumer surplus($\triangle CS$), which can be earned from the recommender system, will be smaller. However, when the expected utility gains from lowering the privacy risk exceeds the $\triangle$CS, personal information concealment will be induced although the correctness of the recommendation drops. Moreover, the increment of consumer ratio, hiding information, will cause the decrement of $\triangle$CS and it will result in accelerating the decision of consumers' information concealing. Accordingly, vicious cycle of RS performance drop and personal information hiding can be started from privacy concerning of consumers.

4. Analysis about Consumer's Decision Making of Personal Information Sharing

Although the users of the recommender system share their personal information in order to receive personal recommendations, they worry about their personal information which may be used inappropriately for other purposes besides the recommendations. According to the Ackerman's survey in 1999, the Internet users concern following four factors mainly when they decide to share their information on the web[12].

- Whether or not the site shares the information with another company or organization.
- Whether the information is used in an identifiable way
- The kind of information collected.
- The purpose for which the information collected.

To decrease the users' worries like these, most web sites ask for the agreement to the users about their collecting information and applying range based on their privacy policies. However, the privacy policies have sometimes been changed, and protective policies on the collected personal information have been retracted, depending on the profits of the web site owners. For example, some of the largest websites, like *Yahoo.com*, have altered their privacy policy to allow them to sell their customers' email address in order to add sources of revenue[13]. As we see from the cases, the right of the users on their personal

information has not been protected in satisfying level, and this fact has been increasing the concerning of users on sharing the personal information.

The most important factor in user's decision about personal information with recommender system is whether the additional consumer surplus, which is created by the recommender system, has larger expected value than expected disutility by sharing their personal information. For modeling this process analytically, we applied followings assumptions.

☐ Assumption 1. The uncertain outcome(X) from purchasing product is a uniformly distributed random variable which exists on [μ_0-σ_0, μ_0+σ_0].

☐ Assumption 2. In case of sharing personal information, recommendation which is provided by recommender system decreases product uncertainty. The changed uncertain outcome($X_{w/r}$) is a uniformly distributed random variable on [μ_0-σ_0, μ_0+σ_0]. ($\sigma_1 \leq \sigma_0$)

☐ Assumption 3. As the rate(k) of the users who share their information in the recommender system increases, the correctness of recommender system increases.

- $\sigma_1 = 1/a \cdot \sigma_0 \cdot (1-k) + (a-1)/a \cdot \sigma_0$ ($a>1$, $1 \geq k \geq 0$)

☐ Assumption 4. As k increases, it decreases the value(C) of disutility from item searching process.

- $C = 1/b \cdot (1-k) \cdot C_0 + (b-1)/b \cdot C_0$ ($b>1$)

☐ Assumption 5. Consumer utility function is assumed to CARA (Constant Absolute Risk Aversion), and consumer utility function of certain outcome(x) is as following. It is assumed to Von-Neumann Morgenstern utility function.

- $u(x) = -e^{-x}$

☐ Assumption 6. Negative outcome which can be made by sharing the personal information is uniformly distributed random variable on [$-2\sigma_2$, 0].

☐ Assumption 7. Each user recognizes the privacy risk differently. For the total user set, the individual value of σ_2 is distributed uniformly on [$-2\sigma_2$, 0].

☐ Assumption 8. The value of C, σ_1 and σ_2 are independent.

Based on the above assumptions, following propositions can be calculated.

☐ Proposition 1. In case of not providing personal information to the recommender system, the expected utility, which comes from product purchasing, is

- $E(u(X)) = u(M_0) = u(\mu_0 - r_0) = u(\mu_0 - \ln((e^{\sigma_0} - e^{-\sigma_0})/2\sigma_0))$
- When $\sigma_0=0$, $r_0=0$
- Risk premium from the uncertainty of product outcome(r_0) is a monotonic increasing function of σ_0.

☐ Proposition 2. In case of providing personal information to the recommender system, the expected utility of purchasing product becomes

- $E(u(X_{w/r})) = u(M_1) = u(\mu_0 - r_1) = u(\mu_0 - \ln((e^{\sigma_1} - e^{-\sigma_1})/2\sigma_1))$

☐ Proposition 3. By providing personal information to recommender system, the uncertainty of product outcome decreases, and the growth of expected utility equals to

- $u(M_1) - u(M_0) = u(\ln((e^{\sigma_0} - e^{-\sigma_0})/2\sigma_0)) - u(\ln((e^{\sigma_1} - e^{-\sigma_1})/2\sigma_1))$
  $= -2\sigma_0/(e^{\sigma_0} - e^{-\sigma_0}) + 2\sigma_1/(e^{\sigma_1} - e^{-\sigma_1}) \quad (\geq 0)$

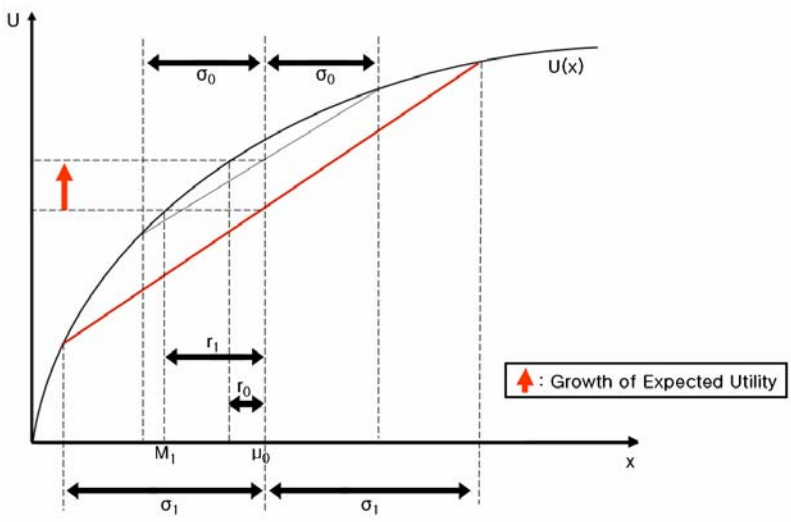

Fig. 1. Growth of expected utility caused by recommendation, according to the decrement of uncertainty in product purchasing

☐ Proposition 4. Expected utility which comes from product transaction, considering the negative uncertainty on the personal information abuse(privacy risk), becomes

- $E(u(X_{w/r,p})) = u(M_2) = u(\mu_1 - r_2) = u((\mu_0 - \sigma_2) - \ln((e^{\sigma_3} - e^{-\sigma 3})/2\sigma_3))$
  $\rightarrow \sigma_3 = \sigma_1 + \sigma_2$

- The outcome of transaction, considering privacy risk is a random variable on [μ_0-σ_1- $2\sigma_2$, μ_0+σ_1] when there isn't searching cost.

☐ Proposition 5. According to the proposition 1, 4 and assumption 4, a user decides to provide personal information to the recommender system when following condition is satisfied.

- $M_2 \geq M_0 - \Delta C$
- ΔC is the decrease of searching cost caused by recommender system.
  → $\Delta C = 1/b \cdot k \cdot C_0$

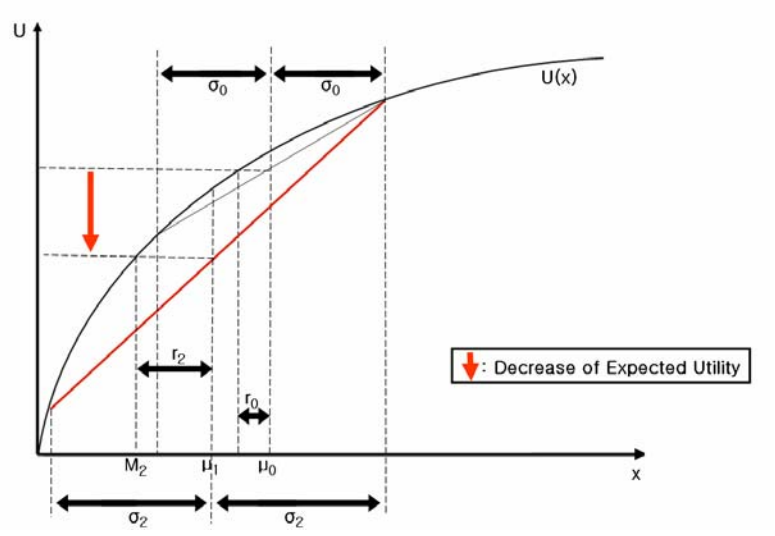

Fig.2. Decrease of expected utility caused by privacy risk, according to the increment of negative uncertainty which comes from privacy risk

As shown in proposition 5, the users share their personal information when the increased expected utility by the recommendation appears larger than the decreased expected utility according to the uncertainty of personal information outflow. On the contrary, when the decreased expected utility because of privacy risk has relatively larger value than the increased expected utility produced by the recommendation, the users will give up the information provided from the recommender system and not share their personal information. Therefore, in order to raise the proportion of personal information sharing, we should be able to enhance the performance of recommender system or reduce the privacy risk of sharing. Finally, we can result in sharing proportion of following proposition 6 from the former assumptions and propositions.

☐ Proposition 6. Based on the proposition 5, assumption 3 and 7, the value of k^*, which is the rate of the users who share their personal information at Nash equilibrium as evolutionary stable state, results in

▪ *When* $k > 0$,

$$\begin{array}{lll} \text{a)} & \text{if } F(k) > 0 & , \quad k^* = 1 \\ \text{b)} & \text{else if } F(k) < 0 & , \quad k^* = 0 \\ \text{c)} & \text{else } (F(k) = 0) & , \quad k^* = \varnothing \end{array} \qquad \text{- (3)}$$

$$F(k) = M_2 - M_0 + \Delta C = A + B \cdot k - \ln(e^{f(k)} - e^{-f(k)}) + \ln(f(k))$$

→ $A = \ln(e^{\sigma_0} - e^{-\sigma_0}) - \ln(\sigma_0)$

→ $B = C_o / b - \sigma_{\max}$

→ $f(k) = (\sigma_{\max} - \sigma_0 / a) \cdot k + \sigma_0$

(3) can be proved by following conditions which is calculated by assumptions and propositions.

When $k = 0$, $F(k) = 0$

When $k > 0$,

$$\begin{array}{lll} \text{a1)} & \text{if } F(k) > 0 & , \quad F'(k) > 0 \\ \text{b1)} & \text{if else } F(k) < 0 & , \quad F'(k) < 0 \\ \text{c1)} & \text{else } (F(k) = 0) & , \quad F'(k) = 0 \end{array}$$

Except the singular case of proposition 6-(c), the value of surplus by recommendation with sharing personal information(*F(k)*) becomes a monotonic increasing or monotonic decreasing function of σ_0, $\sigma_{\max}$, C_o, a and b. When *F(k)* is a monotonic increasing function, the rate of information sharers among the total users becomes the evolutionary stable Nash equilibrium when every user shares their information($k^*=1$). On the other side, when *F(k)* is a monotonic decreasing function, the state of every user not sharing the information($k^*=0$), becomes the evolutionary stable equilibrium.

This shows that the possibility of every user's deciding to share personal information, increases with following circumstances.

- when the decrement of uncertainty increases by recommender system : $\sigma_0 \uparrow$, $a \downarrow$,
- when the decrement of searching cost increases by recommender system : $C_o \uparrow$, $b \downarrow$,
- when the negative uncertainty of sharing personal information decreases : $\sigma_{\max} \downarrow$

This result shows the consistency with the result about the individual's decision making(proposition 5). Of course, all the given assumptions change complex real world to ideal simple situation, and the rate of personal information sharer will have the value between 0 and 1 in reality. However, the basic correlation between, sharing decision and the fitness of recommendation; sharing decision and the privacy risk, will not change. This provides proof intuitions about the necessities for reducing privacy risk without lowering the recommendation fitness.

5. The Weakness of Recommender System in ECommerce Markets

As described before, eCommerce market utilizes recommender system for providing personalized recommendation based on the data which is shared or gathered from consumers. The user pays for the product after he/she makes purchasing decision based on the supporting information, then receives the product from the seller. The figure shows how the information transaction and product transaction happens at the same time in the eCommerce.

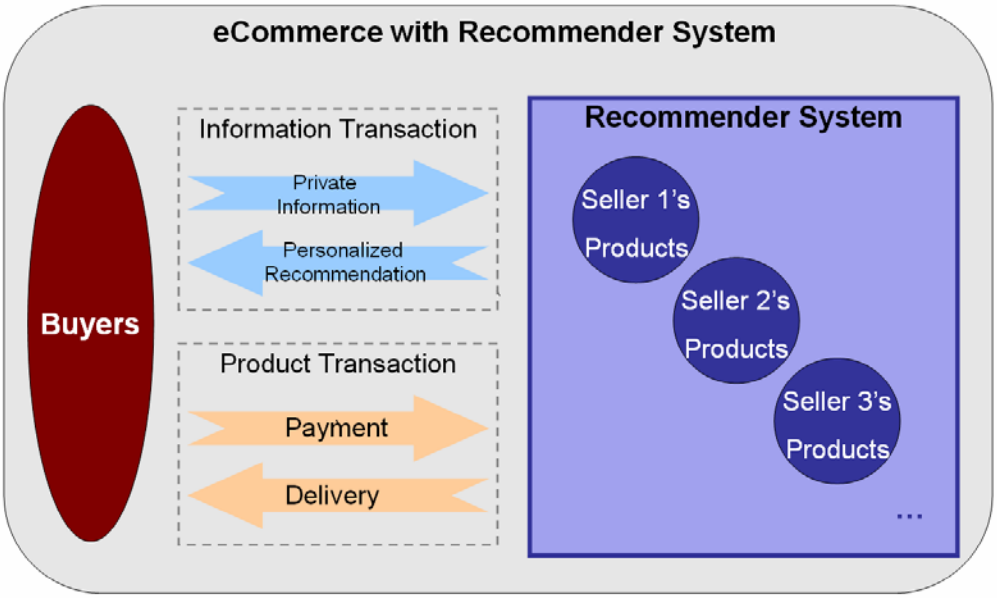

Fig. 3. Information transaction and product transaction in eCommerce with recommender system

In the section 4, we mentioned that in order to promote the eCommerce with recommender system, the risk from sharing personal information needs to be minimized and also needs the fitness of recommendation to be maximized. One of the key factors, for achieving this goal, is to increase the trust between information supplier and demander in online market. The reason is why the trust can decrease the privacy concerning of consumers and increase the fitness of recommendation by easing the aggregation of the truthful personal information. Trust has been considered main issues of online market researches, but purpose of researches have been centered on product transaction. Especially, the researches about reputation have been focused on enabling credible transaction among online market users, having no real contact[14]. However, the decrement of trust in eCommerce causes the uncertainty of the transaction in both cases of information and product transaction. In general eCommerce cases, the difference in trust between product and information transaction is that the risk of product transaction is mainly located in sellers' side, and the risk of information in buyer's side. The reduction of trust will

bring up the cost of both product and information in eCommerce because of risk premium. Consequently, it will bring down the total transaction amount by decreasing surplus which can be gathered by eCommerce activities.

To increase the trust in product transaction between buyers and sellers, eCommerce utilizes the financial or credit institutes for insuring buyers' payment and sellers' delivery. However, in case of information transaction, there are no appropriate systems or institutes to guarantee the trustworthy transaction. Because there is no trust guaranteeing system among sellers, buyers and the recommender systems, there exists high possibility of being exposed to the various attacks. The attacks which are likely to happen can be categorized like below.

☐ Attack by reputation system operator

In June 2001, Sony pictures quoted non-existing movie critic's review for marketing of a new movie, and in case of Amazon it was pointed out that there would be high possibility of the misuse of the recommender system [7]. As we see from those cases, when the recommender system operator gets high profit by making false recommendation, it is likely to happen that the system operator uses the recommender system for malicious purposes. Especially, when it is difficult to distinguish the false recommendation or when the punishment for the false statement does not have compelling power, these problems become more serious. Also the recommender system operator has incentive to sell or share personal information, which was provided for the recommendation, to the companies which are closely related to their own profits.

☐ Attack by product seller.

When the recommender system operator is not the product seller, it is not possible that the product seller makes the false recommendation in order to motivate consumers' purchase. However, the product seller who knows the management algorithm of the recommender system can fabricate the recommendation. It can be one of marketing strategy to generate the false personal information or product preference information for increasing recommendations about their own products. It can also be used for building distrust between the user and the competitive companies. Especially, when there are many substituting products, which have not much difference in the price and quality, these strategies can distort the market permanently by lock-in effect caused by network externality.

☐ Attack by product buyer

When there is not enough trust between the buyer and the recommender system, the product buyer can reject to provide their personal information or provide false information. This attack will drop the efficiency of whole information transaction, and decrease the amount of product transaction by

increasing the uncertainty of item selection at last. Moreover, it is almost impossible to distinguish the false statement from the users. If some part of consumers uses others' personal information to get their necessary information and provide the false information, it will destroy the fairness and generate cross-subsidization among consumers. Consequently, moral hazard and free riding problem will become important in information transaction market. In other words, these attacks from some proportion of users can result in the distrust of all the users because the users who provide true information become to get lower utility from eCommerce than the users provide false. Accordingly, the increment of these attacks can bring out "information lemon market," and this will be serious disaster to recommender systems.

In order to overcome the weakness in information transaction, caused by formerly mentioned attacks, we need various subsidiary mechanisms which secure the trustworthy usage of all the constituents in information market of eCommerce. These subsidiary mechanisms should try to satisfy following basic perspectives.

- Providing the incentive of participating information transaction with trust
- Increasing the cost of attack against recommender system
- Distinguishing the attack and enforcing proper punishment
- Developing the technology or regulatory system for securing the information owner's right
- Inducing the competition on trust as one of the component of service quality

Unfortunately, there is no complete answer for stable operation against all kinds of attacks and satisfying all the above perspectives. Therefore, we need more research effort about this issue before spreading out concerns about privacy risk and malicious attacks. The demand expansion for personalized service is requesting incremental information in online market and this means that the necessity for securing trust in information transaction will be higher in the future.

6. PRINSS – PRivate INformation Shield Service

In this chapter, we will try to suggest new architecture for improving information transaction of current recommender system based on previous studies, which are mentioned in chapter 3. As formerly explained, when anonymous proxy identity is utilized, personal information related with real identity such as payment and delivery is difficult to be protected or aggregated. Surely, the recommender system operator can destroy the information related to real identity right away, but this reduces fitness of recommendation on a large scale by losing important input data of recommender algorithm. Moreover, in reality it is difficult to be done without enforcing regulation with perfect monitoring because this information can be

very important asset for the system operator. On the other hand, if we allow the anonymous identity in the process of payment or delivery, credit payment is impossible and delivery cannot find receiver of the product. In order to solve these problems, we suggest PRINSS-PRivacy INformation Shield Service, which helps to secure both personal information and recommender system input in eCommerce transaction.

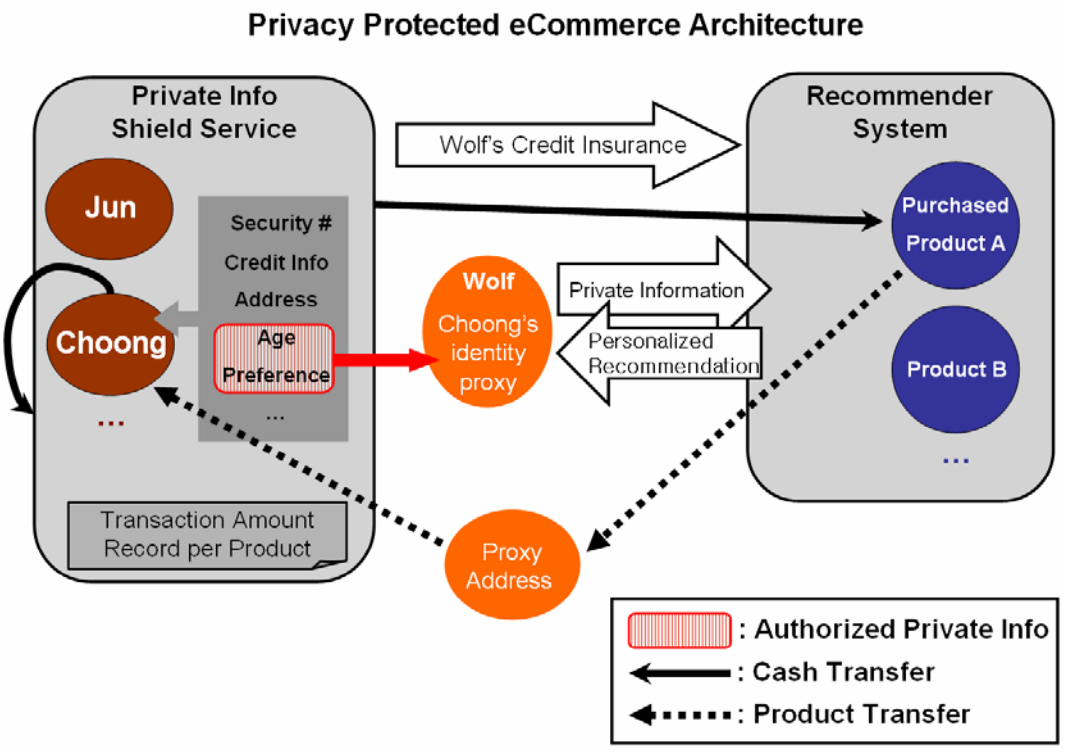

Fig. 4. Privacy Protected eCommerce architecture with Private Information Shield Service

The PRINSS operates as Fig. 3. The figure shows the process of a user named *Choong* buys the *Product A* under PRINSS system. The user who wants transaction in eCommerce forms an identity proxy (wolf, in the figure), and this identity proxy only includes approved personal information which will be shared in the recommender system. Recommender system provides personalized recommendation to the identity proxy based on shared information, and the real user chooses and buys a product based on the recommendation for proxy identity. For enabling credit payment of the identity proxy and delivery to the real buyer, PRINSS provider guarantees the payment and provides proxy address which hides real address to selling side. In other words, PRINSS supports online transaction without showing the actual user during the process related with real identity. Of course, the personal information aggregates to PRINSS provider instead of recommender system or sellers' server, but PRINSS provider has much less incentive to increase specific product sales in online market without the case of colluding. For prohibiting colluding with the product seller, it is important that PRINSS provider is supervised for banning

economic relationship with product seller, and also it is suggested to limit the participation of organizations which can gain high profits from utilizing accumulated personal in malicious ways. Additionally, in order to reduce the risk from the accumulation of personal information in PRINSS, client-side information accumulation technique can be applied. For commercializing client-side accumulation, the PRINSS provider needs to provide privacy agent software, maximizing the convenience of management and the application of identity proxy. Finally, the prohibition of the aggregation for unnecessary personal information to PRINSS provider, such as product purchasing history, preference information, will be appropriate. The personal information, which is accumulated inevitably, should be able to be destroyed according to the service user's request.

In fact, this kind of service can be thought as an expanded form of financial institutes such as bank, credit card companies in the eCommerce. In reality, the provision of PRINSS by financial institutes has several advantages.

- Financial institutes have already accumulated the credit information and the information related with real identity. Accordingly, we need not increase the distribution of personal information.

- In case of financial institutes, we already have strong regulatory agency about their financial activities. This means that we can monitor the PRINSS provider more easily for prohibiting colluding with sellers or recommender systems.

- Financial service institutes have been including customer security as their service quality. Therefore, they have incentive to adopt PRINSS for supplementary service of existing financial services when there are enough demands for PRINSS.

In short, PRINSS can reduce privacy risk with the permanent proxy identity including the history related with real identity, and financial institutes have advantages in realizing PRINSS.

Besides this basic function of PRINSS, which mentioned above, PRINSS also can be functioned as increasing the cost of other attacks to the recommender system by utilizing following subsidiary functions.

- By limiting the sharing of different information for the specific fact of personal information, proxy identity management software can constrain the false information input of users. If we make strong constraints, a user can only generate proxy identity which has truthful personal information. The limiting level can be adjusted considering both users' convenience and recommender system's necessity.

- PRINSS provider can generate the reference for the discrimination of attacks, when the attack is suspicious, from recommender system by recording total amount of product sales. By collecting unsatisfactory report about recommendations or distinguishing the noticeably low acceptance of recommendation, it can check whether these recommendations are made by transparent process or not. To minimize the personal information outflow, client-side software and hardware can be used to determinate attacks.

- PRINSS can increase the cost of generating false information by collecting the product preference or satisfaction only from real product buyers. This function may disrupt to get enough information for efficient management of recommender system. Therefore, by giving the heavier weight to the personal information of real product purchaser, although it uses all the spontaneous information, it can balance the fidelity and the easiness of collecting the information.

- PRINSS can motivate the explicit report such as product preference or satisfaction by giving the direct incentive to the user. The more incentive(cyber money, mileage, etc) is supplied to the reporters who contribute more to the improvement of recommendation fitness. This kind of incentive mechanism can be thought as the application of reputation mechanism. By weighting reports from efficient reporters, we can increase fitness of recommendation and motivate the explicit report of users at the same time. Efficient reporters can are who create reports more strongly correlated with accepted recommendation.

The ways to improve the eCommerce system we mentioned may not be economical solution or can be vulnerable to unforeseen attacks. Therefore, additional effort is necessary to improve the trust in information and product transaction persistently. This effort can be caused by the trust competition among the organizations of eCommerce market to reflect user's request. However, current architecture of eCommerce market does not serve enough roles for this kind of trust competition. Although the demand for technological or regulatory solutions for securing trust among the eCommerce constituents will increase, we need try to develop proper eCommerce system for securing trust to bootstrap trust competition. The success of developed eCommerce system will become clearer when we discover the way of enhancing trust without the deterioration of existing functionality of eCommerce.

7. Summary & Conclusion

Until now, eCommerce grows up based on the B2B market, but as the application of the Internet increases, the relative importance of eCommerce in B2C market becomes important more and more. The biggest

benefit of B2C market is the possibility of personalized marketing and product supply for the users of heterogeneous preference. With this trend, the expansion of product list becomes to require personalized information retrieval services, which can minimize the searching cost and uncertainty of product selection. As the representative solution for satisfying the user's demand about personalization, recommender system of various algorithms are developed and utilized. However, recommender system has not fully reflected the demand about reducing privacy concern. Based on this observation, we tried to provide the basic framework for the economic analysis of recommender system focused on both privacy risk and recommendation fitness. Our analysis shows the importance of the reduction about privacy risk without the deterioration of recommendation. For achieving this goal, we emphasized the trust among eCommerce constituents by enumerating possible malicious attacks when trust was not secured. Finally, we suggested PRINSS-Private INformation Shielding Service for enhancing current information transaction of eCommerce B2C market. Our suggestion applied technological solutions provided by former researchers for reducing privacy risk in recommender system. However, we concentrated more on providing practical architecture reflecting current eCommerce industry. We expect that our research can support existing researches in complementary way, and become one of building block for securing trust in online market. This paper has an important meaning as the starting point for the future research and there must be more additional researches for the improvement of trust in eCommerce.

Reference

1. Lyman, P. and Varian, H. How much information? http://www.sims berkeley.edu/how-much-info, 2000

2. Resnick, P. and Varian, H. Recommender Systems, Communications of the ACM, 1997

3. Goldberg, D. Nichols, D., Oki, B.M., and Terry, D. Using collaborative filtering to weave an information tapestry. Communications of the ACM, 1992

4. Resnick, P., Iacovou, N., Sushak, M., Bergstrom, P., and Riedl, J. Grouplens: An open architecture for collaborative filtering of netnews. Inproceedings of Computer Supported Cooperative Work, 1994

5. Schafer, J. B. ,Konstan, J. and Riedl, J. ECommerce Recommendation Applications, Data Mining and Knowledge Discovery, 2001

6. Ramakrishnan, N., Keller, B. and Mirza, B. Privacy Risks in Recommender Systems, Internet Computing, 2001

7. Lam, S. and Riedl, J. Shilling Recommender Systems for Fun and Profit, Inproceedings of the 13th international conference on World Wide Web, 2004

8. Acquisti, A. and Grossklags, J. Privacy and Rationality Preliminary Evidence from Pilot Data, Inproceedings of 3rd annual Workshop on Economics and Information Security, 2004

9. Cranor, L. F. Laws and application: 'I Didn't Buy it for Myself' Privacy and Ecommerce Personalization, Inproceedings of 2003 ACM workshop on Privacy in the electronic society, 2003

10. Canny, J. Collaborative filtering with privacy. In IEEE Symposium on Security and Privacy, 2002

11. http://www.w3.org/P3P/

12. Ackerman, M. S. and Cranor, L. Privacy Critics: UI Components to Safeguard Users' Privacy. Inproceedings of the ACM Conference on Human Factors in Computing Systems, 1999

13. Miller, B., Konstan, J. and Riedl, J. PocketLens: Toward a Personal Recommender System, ACM Transactions on Information Systems, 2004

14. Resnick, P., Kuwabara, K., Zeckhauser, R. and Friedman, E. Reputation systems, communications of ACM, 2000

15. Bergemann, D. and Ozmen, D. Optimal Pricing Policy with Recommender Systems, Inproceedings of 2nd workshop Economics of Peer-to-Peer Systems, 2004

16. Langheinrich, M. A Privacy Awareness System for Ubiquitous Computing Environments, Inproceedings of 4th International Conference on Ubiquitous Computing, 2002

17. Swearingen, K. and Sinha, R., Interaction Design for Recommender Systems, Inproceedings of Designing Interactive Systems 2002, 2002

18. Varian, H. Microeconomic Analysis 3rd edition, W.W. Norton, 1992