An Analysis of Dynamic Game Strategy of Privacy Protection in Personalization

Li Chen
Guangdong University of Technology, School of management, Guangdong Province, 510520, China, 173404946@qq.com

Hui Zhu
Guangdong University of Technology, School of management, Guangdong Province, 510520, China

Hongwei Liu
Guangdong University of Technology, School of management, Guangdong Province, 510520, China

An Analysis of Dynamic Game Strategy of Privacy Protection in Personalization

Li Chen[1], *Hui Zhu*[2], *Hong-wei Liu*[31]
[1,2,3] Guangdong University of Technology, School of management,
Guangdong Province, 510520, China

Abstract: E-business enterprises provide personalize services for customers based on their privacy information. However, customers benefit from personalization while suffering from privacy concern. The tradeoff between consumers' benefit function and firms' earnings function are explored when an incumbent adopts privacy protection in perfect monopoly market. It also found that when the potential entrant entered into the market, the incumbent that adopted privacy protection can maintain more market shares than one not adopted. At last, we extended this paper and further found that if potential entrant entered into the market with privacy protection would lose more profit because of the large cost of privacy protection. This means the privacy protection that the incumbent adopted has played a certain barriers to entrant.

Key words: privacy protection, personalization, dynamic game strategy

1. INTRODUCTION

The development of information technology and popularity of e-business enable firms to make personalized offers to individual customers through collecting privacy information form customers. For example, Amazon.cn analyze the transaction history of customers and calculate the similarity between customers to provide personalize recommendations[1]. Recently, Gomez et al carried out a study analyzing the organizational privacy practices of the top 50 most visited websites. They found that even though some large and reputable firms like Google, Microsoft, Yahoo and facebook would use customers' privacy information without authorization[2]. Using data in this way causes an associated risk: customers feel more concerns about their privacy. These concerns will affect customers' decisions whether to use personalize services and finally influence the profit of enterprises, which would cause personalization-privacy tradeoff[3, 4]. The game theoretic on personalization has shown that personalization based on personal information not only can cause competition [6, 7], but also can solve the contradiction of personalization-privacy. Results of this study can make incremental contributions to the existing literature.

2. LITERATURE REVIEW

Privacy protection was essentially divided into two categories: one was the technical aspect of privacy protection algorithm. The other was the legal aspect of privacy protection policy. We summarized literatures from these two aspects as below.

2.1 Privacy Protection Algorithm

In recent studies, they mainly focus on the algorithm of data mining, especially the association rules algorithm of privacy protection. According to the data storage, algorithm of privacy protection can be divided into two broad categories: privacy protection technology for centralized data set and for distributed data. The main technologies of centralized data set of data mining are attributes changing, blocking and random response. For example, Agrawal proposed ID3 decision tree of privacy protection based on interference[8]. This method adds random value to original data. Then, it calculates the density function of original data via Bayes formula so

[1] Corresponding author. Email: 173404946@qq.com

that it can rebuild the decision tree. Weiping Ge et al based on the transition probability matrix to translate the attributes of data. Thus generate the decision tree by restoring property values from the data translated before[9]. Alexandre showed using a random operator called "select-a-size" to translate the primary data. Then randomly and independently transformed each record and used these data translated to calculate the support of item set [10]. Distributed data mining is a popular method at present, and its privacy protection algorithm is mainly based on secure multi-party computation. This method can ensure that each computer just product specified output but not getting other information. Clifton provided four algorithms of secure multi-party computation: secure sum, secure set union, secure size of set intersection and scalar product[11].

2.2 Privacy Protection Policy

The main protocols of privacy protection are Fair Information Practices (FIPs) and The Platform for Privacy Preferences (P3P). FIPs are a set of standards governing the collection and use of personal information. They are based on five core principles: notice, choice, access, security and enforcement[12]. Customers will trust a firm who implements the FIPs and willing to provide privacy information to firms[13]. P3P framework, a privacy protocol that standardizes privacy policy information to allow user to gain a better understanding of how websites' privacy policies match their action involved users' privacy[14, 15]. A privacy enhancing technology named Privacy Bird uses a notification process to inform a user browsing the Internet about how privacy friendly a website is[14, 16].

2.3 Problem Existed

Although there are all kinds of privacy protect algorithm, a large number of empirical studies confirmed that most of this algorithms were not accepted by consumers. For consumers, these algorithms are difficult understood. In addition, most of these algorithms are only conceptual frameworks and it is difficult to convert to actual tools. However, privacy protection policy, such as FIPs, often lack of legal authority. Companies still do not provide privacy protection for consumers and when they, they often do not comply with the FIPs standards[17-21]. The primary cause of these problems is that they cannot prove how these algorithms and policies relate to the interests of consumers, and how to comply with the profit maximization principle of firms. If using game theory, it can be calculated the gains consumers got and the profit firms earned. Then it is found the balance between the gains got after consumers giving their privacy information and the profit earned after firms implementing the privacy protection. This model considers oligopoly market as an example, and explores the market competition between incumbent firm A and potential entrants firm B. If firm A as an incumbent implements privacy protection, what kind of privacy concern level that a consumer holds will be affected? Firm B as a potential entrant, how will it be influenced? It will be discussed in the following chapters.

3. MODELING

In this chapter, a complete monopoly market model is developed and the model is evolved after the potential intruder entering the market. In this study, complete monopoly market means seller's monopoly. In other word, there only exists one firm in a market[22]. The purpose of establishing these models is to calculate the payoff function of incumbents and potential entrants in monopoly market so that it can provide support for establishing dynamic game of complete information.It is assumed that firm A is in a complete monopoly position while firm B is a potential entrant in a market. Either in complete monopoly market or in competitive market, consumer will buy product from firm A or firm B.

3.1 Two dimensions of the model

This model has two dimensions: consumers' preferences and privacy concern level.

3.1.1 Consumers' preferences

As is known to all that consumers have different preferences which are difficult to be change. For example, some females prefer red lipstick while some prefer orange lipstick. If consumers have the same preference, the market will be simplified which will not happen in reality. One of dimensions in this model is preference. It is assumed that consumer preferences are uniformly distributed on the line [0,1]. Each consumer in this market can be viewed as a point on the line which represents their preferences. R represents the value that consumers' reservation value for their ideal product. Since every consumer has their own ideal product, x represents the distance between the location of the consumer's ideal product and the location of the product in the line. Meanwhile tx means a value of loss when consumers buy a real product, which t expresses consumer's preference coefficient.

3.1.2 The classification of consumers' attitude to privacy

Smith. H Jeff states it clear that what privacy concern is in his article[23]. The reasons which cause privacy concerns are various. For example, the differences of personality, person who is introversion may feel more concern about their privacy than the extroversion[24]. People who is independent may feel different degree of concerns about his privacy[25]. Five types of personality characteristics also have different to privacy concerns[26]. It can classify people into three kinds according to their different attitudes to privacy: the unconcerned, pragmatists and fundamentalists[27, 28]. One of the dimensions of our model is the classification of consumers' attitude to privacy which is consisted by these three kinds of people.

Fundamentalists have strong self-protection awareness and they are not willing to reveal any privacy information to any enterprises. For these reason enterprises cannot collect their information. However, the unconcerned do not care about their privacy, so enterprises can easily collect their information. The third people are pragmatists who provide their information depended on what the situation they are in. If the pragmatists know the enterprise can take privacy protection such Platform for Privacy Preference (P3P) or Fair Information Practices (FIPs) to protect their information when providing services, they are willing to share information to enterprise. Otherwise, they will not share information[23]. A recent survey of 1000 adults in the United States by Westin and Harris Interactive found that the percentage of fundamentalists, pragmatists and the unconcerned are respectively 26%,64% and 10%[29]. To simplify the model, the sizes of the unconcerned, pragmatist, and fundamentalist segments are respectively denoted as $u, v, w(1-u-v)$,and $v > u$ .Figure 1 shows the situation about these three kinds of people sharing their information.

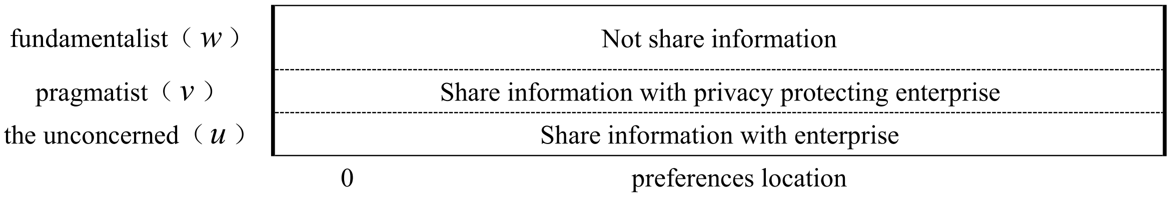

Fig. 1. Market Segment

3.2 Product and target market

3.2.1 Standard product of firm

Suppose there is an incumbent, firm A, and a potential entrant, firm B in perfect monopoly market. Both of them can product different standard products and provide personalization products in certain scope[30]. To simplify the model, assume marginal costs of firms are 0, which means production will not cause any loss. Both firm A and firm B can price their standard products. P_i denote the price of firm *i*'s standard product, where *i=A or B*. As mentioned in section 3.1.1, let R denote the consumers' expected value of ideal product and tx denote the value of loss when consumer buy real product compared to the ideal product. Then the net value of buying standard product is $R-P_i-tx$, and $P_A > P_B$.

3.2.2 Personalized product

Firms offer personalized products to consumers on the basis of information collected. Amazon.com can provide personalized recommendations which use collaborative filtering to recommends books, music and other products[1] . Firms offering personalized services are based on information of consumers. For this reason, personalized services involves in consumers' privacy. As mentioned above, people have different attitudes to their privacy and they may accept or not firm's service. Fundamentalists only buy standard products, because they won't share any information to firms and also cannot get any personalized services. Pragmatists will accept personalized product when firm protecting privacy, otherwise they will choose standard product. The unconcerned can buy standard product or personalized product because they don't care about their privacy and firms can easily collect their information and take use of it. We suppose the personalized product bought by consumer will completely fit to their preferences [7]. Assume that marginal cost of personalized product is 0 [30]. Personalized scope of a firm is defined as inside the preference line [0,1] in which firm produces products. However, personalized scopes of firms are limited because of the restrictions of technology and capital. In this model, S denotes the personalized scope of a firm and $p_i(x)$ respects price of personalized product, where i =A or B.

3.3 Cost of privacy protection

Protect privacy will lead to cost which is consisted of fixed cost and variables cost. Fixed cost which denoted by K_p refers to necessary cost for protecting privacy, such as training fee and system structuring fee. The other is variable cost which depends on the consumers' attributes to their privacy. Previous research shows that it will be more expensive to collect information of people with higher sensitivity of privacy than the one with lower sensitivity. In this model, assuming K_i^u denotes cost of collecting information of the unconcerned, where i =A or B. The concerned have lower sensitivity of privacy, so collect information of them won't cost much. K_i^{u+v} denotes the cost of collecting information of pragmatist and fundamentalist, where i =A or B.

3.4 The sequence of firms' strategy in game

This model involves to two firms, firm A which is an incumbent and firm B which is a potential entrant. In dynamic game theory, participants' actions are in sequences and the latter can see the former's strategy. In this model, firm A takes an action first and firm B makes a decision after knowing firm A's decision. Firm A will decides whether carry out the protection of privacy firstly. Then, firm B decides whether enter the market or not. Thus, strategy space of firm A is （pro-not pro） which is denoted by S_A. Firm B has two sets of decisions and each set has two choices, which means firm B has four pure strategies: {pro, enter}, {pro, not-enter}, {not-pro, enter}, {not-pro, not-enter}. Figure 2 shows the tree of game.

4. COMPETITION IN MONOPOLY MARKET

To determine the subgame perfect Nash equilibrium of game model of privacy protection used backward induction, we should divide the target markets of firms based on consumers' preferences and their attitudes to privacy and figure out the revenue functions of the firms according to their product prices.

Assuming the percentage of people who are willing to share information with firm A is α and percentages of one who will share information with firm B is β. As potential entrant, it is difficult for firm B to collect pragmatists' information in a short time and cost of collection will be high after firm B entering[6]. Because firm A is in monopoly position, it can collect consumers' information from transaction happened before and from consumer information database which accumulated in a long time. For these reasons, cost of collection from firm B is higher than that from firm A. However, in database of firm A, it cannot be distinguished the unconcerned and pragmatists.

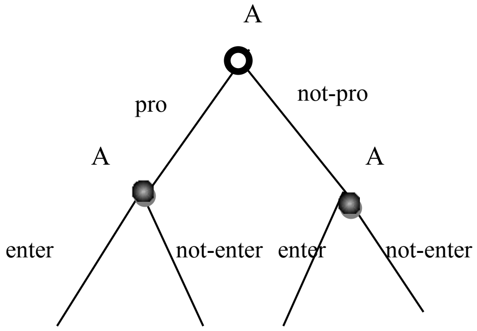

Fig. 2. Game model of privacy protection

4.1 Firm A protect privacy while firm B enter the market

The first case is that firm A protects privacy and firm B decides to enter the market. Since firm A provides protection for privacy, the person who are willing to share their privacy are $\alpha{=}u+v$. While firm B only get information of β, where $\beta=u$. As mentioned before, the scope of personalized services of firm is limited. Assume that personalized scope of firm A is $[0,S]$ and personalized scope of firm B is $[1\text{-}S,1]$, where $S>\frac{1}{2}$. After firm A implementing the privacy protection and the entrance of firm B, the market is divided as the figure 3 showed.

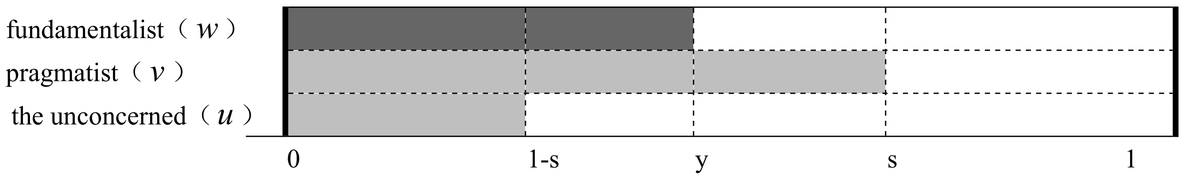

Fig. 3. {pro, enter}, target market of firms

The dark shadow areas denote the target market of firm A offering standard product and the whiter shadow areas denote the target market of firm A offering personalized product. The white areas denote firm B's. The shadow areas are target markets of firm A after firm B entering the market. Suppose $P_A{+}ty=P_B+t(1-y)$, where $y=\frac{1}{2}+\frac{1}{2t}(P_B-P_A)$. When $1\text{-}S\leq y\leq S$, equilibrium point will exist between these two firms which can refer Dong-Joo Lee(2011)[21]. The area of $[1-S,S]$ is the range where two firms compete for consumers. Assuming a consumer is locating in position x. This consumer can buy personalized product or standard product from firm i, so his net utility is $\max\left[R-p_A-tx,R-p_B-t\left(1-x\right)\right]$. Thus, only when net utility equals $\max\left[R-p_A-tx,R-p_B-t\left(1-x\right)\right]$, will consumers choice products of firm i .The price of personalized products is $q_i\left(x\right)$ （ $\equiv\left[p_A+tx,p_B+t\left(1-x\right)\right]$ ）. Under this price, consumer can get most benefit, while firm i can also reach the maximal profit. Consumers will choose personalized product rather than standard one when the benefits of them are the same. Assuming profit of firm A is π_A^1 and profit of firm B is π_B^1. The payoff functions are as followed:

$$\pi_A^1{=}\alpha\int_0^{1\text{-}S}P_A+txdx+(\alpha-\beta)[\int_{1-S}^{y}P_A+txdx+\int_y^S P_B+t(1-x)dx]+(1-\alpha)\int_0^y P_Adx-K_p-K_A^{u+v}$$

$$\pi_B^1=\beta\int_S^1 P_B+t(1-x)dx+\frac{\beta}{\alpha}(\alpha-\beta)[\int_{1-S}^y P_A+txdx+\int_y^S P_B+t(1-x)dx]+(\alpha-\beta)\int_S^1 P_B dx+(1-\alpha)\int_y^1 P_B dx-K_B^u$$

4.2 Firm A protect privacy without firm B's entering

The second case is that firm A protects privacy without firm B's entering. In this case, firm A is still in the monopoly position. When firm A protects privacy, it can provide personalized scope for pragmatists, then $\alpha = u + v$, $\beta = 0$. Figure 4 is the target market of firm A in the second case. The dark shadow areas are the market of offering standard products, and the whiter shadow areas are the market of offering personalized products. Then it can be calculated the profit of firm A π_A^2:

$$\pi_A^2=\alpha\int_0^S P_A+txdx+\alpha\int_S^1 P_A dx+(1-\alpha)\int_0^1 P_A dx-K_p-K_A^{u+v}$$

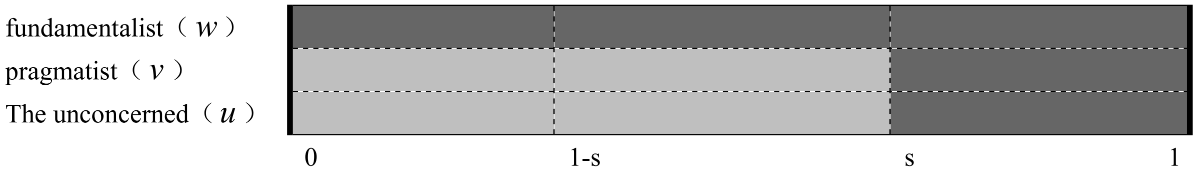

Fig. 4. {pro, not- enter}, target market of firms

Because firm B doesn't enter the market, its profit is $\pi_B^2=0$.

4.3 Firm A doesn't protect privacy with firm B's entering

The third case is that firm A doesn't provide privacy protection, while firm B enters the market. In this case, firm A only can offer personalized products to the unconcerned and provides standard products to pragmatist and fundamentalists, $\alpha = u = \beta$. Similarly, it is assumed that $P_A + ty = P_B + t(1-y)$, where y denotes diffident location of consumer. Figure 5 is the target market in third case. The shadow areas are target markets of firm A after firm B entering. The dark shadow areas are offering standard products while the whiter shadow areas are offering personalized products. The white areas are market of firm B.

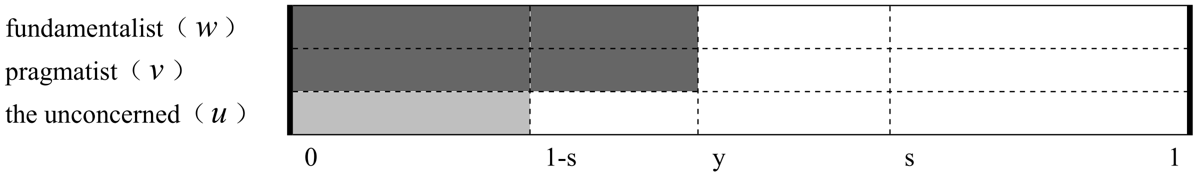

Fig. 5. {not-pro, enter}, target markets of firms

The profits of firm A and firm B are as followed.

$$\pi_A^3=\alpha\int_0^{1\text{-}S} P_A+txdx+(1\text{-}\alpha)\int_0^y P_A dx-K_p-K_A^u$$

$$\pi_B^3=\beta\int_y^1 P_B+t(1-x)dx+(1-\alpha)\int_y^1 P_B dx+\beta\int_{1-s}^y P_A+txdx-K_B^u$$

4.4 Firm A doesn't provide protection without firm B's entering

The forth case is that firm A doesn't provide protection, while firm B doesn't enter. Firm A provides personalized products to the unconcerned, also provides standard products to pragmatists and fundamentalists, which means $\alpha = u = \beta$. Figure 6 shows the target market in this case.

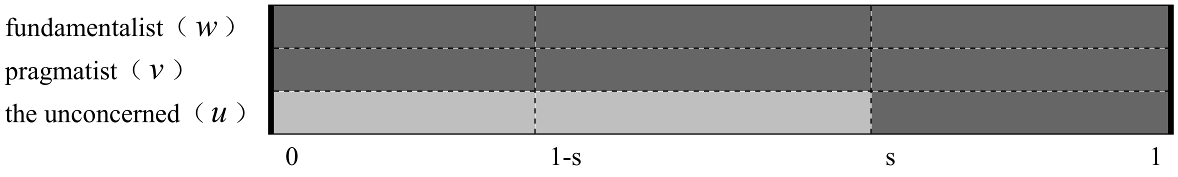

Fig. 6. {not- pro, not-enter}, target market of firms

The profit of firm A as followed function.

$$\pi_A^4=\alpha\int_0^S P_A+txdx+(1-\alpha)\int_0^S P_A dx+\int_S^1 P_A dx-K_A^u$$

Meanwhile, because firm B doesn't enter, its profit is $\pi_B^4=0$.

5. CONCLUSION

The payoff functions are showed in previous chapter. The results can be gotten as followed through calculating:

Compare the profit of these four cases:

$$\pi_A^2-\pi_A^3=\frac{t}{2}(2P_Atus+vs^2t^2+tvP_A+(1-u-v)P_A+(2ust^2-ut^2)+(1-u)(P_A^2-P_AP_B))>0$$

$$\pi_A^1-\pi_A^2=(ut^2-2ut^2s)+(vt^2-2vt^2s)+(2P_Ast-2P_Astu)+(P_AP_B-P_A^2)-2tvsP_A-$$

$$P_Atv-P_Btv-\frac{1}{2}P_B^2v-2t^2vs^2-vP_A-\frac{3}{2}P_A^2v-\frac{3}{2}t^2v<0$$

$$\pi_A^2-\pi_A^4=\frac{1}{2}vts^2+K_A^u-K_p-K_A^{u+v}<0$$

$$\pi_A^3-\pi_A^1=-\frac{1}{2t}(\frac{1}{2}v(P_A-P_B)+t^2s^2v+stvP_B+\frac{1}{2}t^2v)<0$$

So the profit of these four cases are $\pi_A^3<\pi_A^1<\pi_A^2<\pi_A^4$ and $\pi_B^2=\pi_B^4<\pi_B^3<\pi_B^1$. Thus, the sub-game refining Nash equilibrium result is (π_A^1,π_B^1), which is {pro, enter}. The following will be the conclusions of different cases.

(1) In the forth case {not- pro, not-enter}, firm A is in the monopoly position. If firm B doesn't enter, firm A is not necessary to carry out the protection of privacy. However, in the second case {pro, not-enter}, although firm A protecting privacy can attract pragmatists to buy their personalized products, it also causes a series of cost which results the lower profit. This phenomenon indicates that when firm A is in monopoly market, it is not necessary to carry out the protection because of lacking competitors.

(2) In order to maximize its profit, firm B will enter the market to compete for consumers. However, because of the limited time, firm B cannot collect the information of pragmatists, which means it won't carry out the protection. Meanwhile, firm A should carry out the protection so that it can collect large among of consumers' information and increases more investment to provide personalized services. For these reason, firm A will attract pragmatists to buy its personalized products and get more exact profit. Then firm A can reduce the investment and competition for the unconcerned, avoid the price competition with firm B and maximize the profits of both sides. Otherwise, if firm B enters the market and firm A doesn't provides protection, then the two firms would compete for the unconcern, which may causes price competition and jeopardize the interests of two firms.

(3) Assume that firm B collects information of pragmatists before it entering the market, so it will compete with firm A for the unconcern and pragmatists after entering the market. However, because firm A is a monopolist, it can accumulate information of consumers through trading with consumers, mining consumers' web browsing. Firm B doesn't have these accumulation, so the cost of protection of firm B will be more than that of firm A, $K_B^{u+v}>K_A^{u+v}$. If firm B enters the market and insists providing protection, it may not only cause price competition but also increases the cost of firm B.

(4) To the consumers in this model, their profit can be maximized and their requirements for standard products or personalized products can be satisfied. Pragmatist can share their information depend on whether firms provide privacy protection or not. Fundamentalists can choose standard products to satisfy their needs. In this situation, interests of consumers and profit of firms can get the balance.

ACKNOWLEDGEMENT

This research was supported by the National Natural Science Foundation of China under Grant 70971027.

REFERENCES

[1] Acquisti, A., Varian, H.R.(2005). Conditioning prices on purchase history. Marketing Science 24, 367-381.

[2] Agrawal, R., Srikant, R. (2000). Privacy-preserving data mining. ACM Sigmod Record 29, 439-450.

[3] Arora, N., Dreze, X., Ghose, A., Hess, J.D., Iyengar, R., Jing, B., Joshi, Y., Kumar, V., Lurie, N., Neslin, S., (2008). Putting one-to-one marketing to work: Personalization, customization, and choice. Marketing Letters 19, 305-321.

[4] Awad, N.F., Krishnan, M.(2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS quarterly, 13-28.

[5] Belanger, F., Hiller, J.S., Smith, W.J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. The Journal of Strategic Information Systems 11, 245-270.

[6] Blattberg, R.C., Kim, B.-D., Neslin, S.A.(2008). Database marketing: analyzing and managing customers, Springer Verlag, Vol 18.

[7] Chen, Y., Iyer, G., 2002, Research note consumer addressability and customized pricing. Marketing Science 21, 197-208.

[8] Chen, Y., Narasimhan, C., Zhang, Z.J.(2001). Individual marketing with imperfect targetability. Marketing Science 20, 23-41.

[9] Choudhary, V., Ghose, A., Mukhopadhyay, T., Rajan, U.(2005). Personalized pricing and quality differentiation. Management Science 51, 1120-1130.

[10] Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., Zhu, M.Y.(2002).Tools for privacy preserving distributed data mining. ACM SIGKDD Explorations Newsletter 4, 28-34.

[11] Cranor, L.F.(2006).What do they indicate: evaluating security and privacy indicators. Interactions 13, 45-47.

[12] Cranor, L.F., Guduru, P., Arjula, M.(2006). User interfaces for privacy agents. ACM Transactions on Computer-Human Interaction (TOCHI) 13, 135-178.

[13] Culnan, M.J., Bies, R.J.(2003).Consumer privacy: Balancing economic and justice considerations. Journal of social issues 59, 323-342.

[14] Dewan, R., Jing, B., Seidmann, A.(2003). Product customization and price competition on the Internet. Management Science 49, 1055-1070.

[15] Evfimievski, A., Srikant, R., Agrawal, R., Gehrke, J.(2002). Privacy preserving mining of association rules. In: Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining, 217-228.

[16] Robert Pitofsky. (2000)Fair Information Practices in the Electronic Marketplace. A Report to Congress.

[17] Gomez, J., Pinnick, T., Soltani, A.(2009). KnowPrivacy. The Current State of Web Privacy, Data Collection, and Information Sharing. School of Information, University of California Berkeley

[18] Interactive, H.(2002).Privacy On and Off the Internet: what consumers want. Privacy and American Business, 1-127.

[19] Jensen, C., Potts, C.(2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. In: Proceedings of the SIGCHI conference on Human factors in computing systems, 471-478.

[20] Kasanoff, B. (2001). Making it Personal: how to profit from personalization without invading privacy.

[21] Lee, D.-J., Ahn, J.-H., Bang, Y.(2011). Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection. MIS Quarterly-Management Information Systems 35, 423.

[22] Linden, G., Smith, B., York, J.(2003). Amazon. com recommendations: Item-to-item collaborative filtering. Internet Computing, IEEE 7, 76-80.

[23] Liu, C., Arnett, K.P.(2002). Raising a red flag on global WWW privacy policies. Journal of Computer Information

Systems 43, 117-127.

[24] Lu, Y., Tan, B., Hui, K.-L.(2004). Inducing customers to disclose personal information to internet businesses with social adjustment benefits.

[25] Narasimhan, C.(1988). Competitive promotional strategies. Journal of Business, 427-449.

[26] Peslak, A.R., (2005a). Internet privacy policies: a review and survey of the Fortune 50. Information Resources Management Journal (IRMJ) 18, 29-41.

[27] Peslak, A.R., (2005b). Privacy policies of the largest privately held companies: a review and analysis of the forbes private 50. In: Proceedings of the 2005 ACM SIGMIS CPR conference on Computer personnel research, 104-111.

[28] Peslak, A.R.(2006).Internet privacy policies of the largest international companies. Journal of Electronic Commerce in Organizations (JECO) 4, 46-62.

[29] Reagle, J., Cranor, L.F.(1999). The platform for privacy preferences. Communications of the ACM 42, 48-55.

[30] Shaffer, G., Zhang, Z.J.(1995). Competitive coupon targeting. Marketing Science 14, 395-416.