Electronic Commerce Research and Applications 9 (2010) 435–445

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

journal homepage: www.elsevier.com/locate/ecra

An economic model of optimal fraud control and the aftermarket for security services in online marketplaces

Seonyoung Shim [a,*], Byungtae Lee [b]

[a] Department of Business Administration, College of Social Science, Seoul Women's University, 623 Hwaragno, Nowon-gu, Seoul, Republic of Korea
[b] Graduate School of Business, Korea Advanced Institute of Science and Technology (KAIST), 207-43, Cheongryangri2-dong, Dongdaemun-gu, Seoul, Republic of Korea

ARTICLE INFO

Article history:
Received 18 December 2008
Received in revised form 3 August 2009
Accepted 3 August 2009
Available online 12 August 2009

Keywords:
Analytical model
Consumer privacy
Economic theory
Information asymmetry
Online fraud
Privacy controls

ABSTRACT

The anonymity of online markets allows traders to easily behave opportunistically. Online marketplaces can lower the uncertainty of participants' identities by adopting preventative controls such as privacy disclosure rules. However, the use of severe privacy controls to engender risk-free environments might sacrifice not only the size of transactions in the marketplace but also the demand for optional security services like escrow services, which constitute a very sizable revenue source for the marketplace services provider. In this vein, we investigate the probability that an integrated online marketplace (IOM) with security services strategically adjusts privacy controls to incentivize traders to self-select both basic transactions and optional security services. Our results show that an integrated marketplace increases the probability of allowing more fraud than is socially optimal by lowering privacy controls. Market risk can be viewed as an asset for an integrated marketplace rather than a liability that inflicts transaction costs on worried traders. Our study argues that marketplaces may differ in terms of their fraud control from what is socially optimal, according to their revenue structures so that the control of online fraud needs to be regulated from the social perspective. However, under certain conditions, integration of this aftermarket will not harm traders or the social welfare.

1. Introduction

Creating markets is a mainstay of dotcom business models (Kambil and Heck 2002). While the extensive listings of tradable goods and powerful search technologies make online markets liquid,[1] the electronic media connecting trading participants and sharing quality information remains lean. With direct trades between unknown customers over great distances, online transactions are vulnerable to many types of fraudulent conduct.[2] The main reason that the online marketplace easily attracts fraud originates from a unique characteristic of Internet transactions. Under considerable *information asymmetry* – the uncertainty of trader identity and the uncertainty of merchandise quality – online trade allows sellers or buers to easily engage in opportunistic behavior (Klein and Leffler 1981).

One way to directly resolve fraudulent actions in anonymous markets is lowering the uncertainty of identity through disclosure of private information, which makes individuals identifiable (Culnan and Armstrong 1999). The anonymity of the Internet is a double-edged sword, however. Honest traders may prefer this characteristic for the protection of their privacy, while opportunistic people take advantage of it to commit fraud. If the practices of an online business raise privacy concerns resulting in a perception that customers must reveal too much personal information or that the information may be used unfairly, customers unwilling to disclose additional personal information may spread bad word-of-mouth (Culnan and Armstrong 1999). The result may be that businesses will have difficulty attracting new customers, which can negatively impact the bottom line.

Online marketplaces need to do a very tricky balancing act, mitigating the opportunity costs of electronic transactions that result from anonymity while protecting the privacy of the majority of their customers. This issue presents possible conflict between strict security control and infringement of consumer privacy, as

* Corresponding author.
E-mail addresses: seonyoungs@swu.ac.kr (S. Shim), btlee@business.kaist.ac.kr (B. Lee).

[1] The online auction is a representative business model that illustrates how a business can be changed with the aid of new technologies. Successfully serving C2C transactions, online auctions have grown at a remarkable rate and become a major consumer channel. There is no doubt of this in terms of the number of items registered and traded, amount of sales, and trading profits. For example, eBay – the world's largest online auction company, which services 29 international markets – reported 309.3 M registered users and 647.4 M new product listings, a net revenue of $2.1 B and a gross merchandise volume (GMV) of $16,036 M for the first quarter of 2008 (eBay Reports 1st Q 2008). This dramatic online market liquidity comes from a variety of opportunities for consumers that are not offered offline.

[2] Fraudulent transactions in online marketplaces involve shilling, bid shielding, misrepresentation, fee stacking, failure to ship/pay, reproductions and counterfeits, triangulation/fencing, buy and switch, loss or damage claims, and sell auctions (Chau and Wareham 2004).

1567-4223/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.elerap.2009.08.003

discussed by prior studies (Culnan and Armstrong 1999, Rowland 2000). However, we go further by identifying the business value of security services (e.g., escrow services) for online marketplaces and explore the possibility that market risk is intentionally under-controlled and strategically utilized according to the revenue structure.

We pay attention to the fact that security services that insure traders against transaction risk may not only be good *ex post* measures against the risk of online fraud but also a very sizable revenue source for online marketplaces. For example, eBay integrated both trading and escrow services when it took over PayPal in July 2002 and eBay's recent good business performance is largely attributed to PayPal (Cullen 2007).[3] Note that imposition of excessively austere privacy controls not only incites online users' privacy concerns but also gives them less incentive to adopt security services due to reduced market risk (Antony et al. 2006, Zhang et al. 2007). However, loosely controlled market risk brings about more opportunity for online fraud. Therefore, when an online marketplace provides in-house security services along with basic transaction services, its decision on the preventative privacy controls is complicated by the issues of privacy concern and the promotion of security services.

We are primarily concerned with how the integration of transaction and security services distorts online market decisions on privacy controls from social optimality. In other words, this study examines the conditions under which the provision of security services should be integrated with an online marketplace or independently managed by third parties. Given that online commerce is claiming a rapidly growing share of worldwide business, and customers have concerns about security and privacy, we believe that this is a very pressing research question.

2. Theoretical background

2.1. The economics of preventative fraud control and ex post security measures

For the control of crime, we find two alternatives from the criminal sociology literature (Gopal and Sanders 1997) – preventative measures and deterrent controls. The former increases the *ex ante* cost of crime by dissuading potential offenders from crimes in the first place, while the latter dissuades criminal intent with the *ex post* threat of legal sanctions, which are costly. Thus, the socially optimal choice of controls will be those that minimize the social loss from crime – the sum of damages and the cost of preventative and deterrent controls (Becker 1968). Based on this economic perspective of crime, IS studies illuminate the cost of preventative controls in cases involving software piracy. Although it is believed that anti-piracy measures increase software firm profits, the studies argue that software piracy should not be strictly prevented because such prevention leads to a reduction in the size of the user base (Conner and Rumelt 1991, Gopal and Sanders 1997).[4]

The same issue exists in the control of market risk. All marketplaces – including online markets – operating under information asymmetry share the risk of fraud (Akerlof 1970). Markets require some form of security measures and have embraced various risk-relief measures corresponding to different types of uncertainty. First, combinations of various remedies for the "lemon" problem reduce the risk from the *uncertainty of product quality*: reputation (Heal 1976, Kreps et al. 1982, Lynch et al. 1986), advertising (Lynch et al. 1986), and serving selective customers through credit-rationing (Stiglitz and Weiss 1981). Other security measures such as online escrow services or debit accounts (Hu et al. 2004, Zhang et al. 2007) primarily reduce the risk from the *uncertainty of identity*.

Although such indirect measures may make the problem less acute, complete elimination of the information asymmetry problem is beyond their reach, while direct disclosure of information carries the cost of deteriorating the potential user base. Therefore, transactions with a certain degree of uncertainty require both the imposition of preventative controls and complementary *ex post* security measures. Especially when the marketplace embraces optional revenue sources related to such controls, the optimal enforcement of privacy controls and its impact on the additional security measures is worthy of investigation.

2.2. Warranties and mechanism design

In the online marketplace, traders who want to avoid the risk of fraud optionally adopt security services. For simplicity of analysis, in this study the level of preventative privacy control means the level of preventative privacy disclosure, which captures the conflict between preventive security control and privacy concerns. We denote the level of privacy control in the marketplace by α^m. This and all other notation that we use in this article are defined and discussed in Table 1 (See Appendix A). Fig. 1 shows the principal characteristics of the integrated provision of transaction and security services.

First, the integrated online marketplace (IOM) provides a basic service for transactions, $Q_t(\alpha^m)$, and the optional (security) service for risk prevention, $Q_s(\alpha^m)$. Overly strict privacy controls directly affect the demand for basic services due to the disutility derived from privacy disclosures. *Second*, while privacy disclosure is not directly required for the adoption of a security service, it is partially an economic substitute for a security service. The decrease in fraudulent activities in the marketplace lowers the incentives to adopt the security service. Hence, the imposition of severe preventative privacy controls to engender risk-free environments might sacrifice not only the demand for the primary service but also that for the optional security service. *Third*, the demand for online transactions, $Q_t(\alpha^m)$, and the bundled final service, $Q(\alpha^m)$, are not straightforward, even though they depend on α^m, due to heterogeneous consumer distribution in risk attitude and the possibility of opportunistic transactions. Hence, the aforementioned relationships make strategic control of IOM complex.

For an IOM, security service is a means to shift risk-averse traders to risk-neutral ones. Thus, we find that the underlying characteristics of our model are quite similar to the features of extended warranty studies (Padmanabhan and Rao 1993, Lutz and Padma-

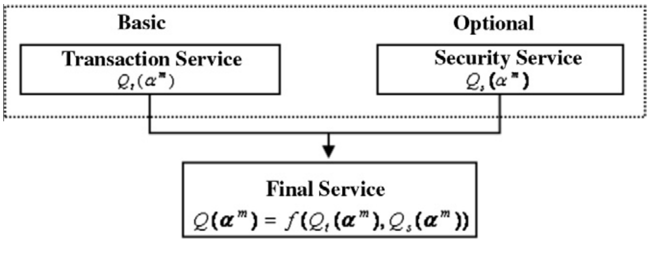

Fig. 1. Transaction and security services in the marketplace.

[3] In 2006, PayPal's net revenue constituted about 33.6% of eBay's online marketplaces, and it increased to 37.9% by the 4th quarter of 2007. In 2008, PayPal operated in 190 markets and manages more than 164 million accounts. PayPal allows customers to send, receive and hold funds in 19 currencies worldwide. See http://en.wikipedia.org/wiki/Paypal.

[4] Conner and Rumelt (1991) shows that under positive network externalities, no protection is optimal for the firms and consumers. Increased protection raises the cost of pirating, thus causes some pirates to buy or to give up using the software. This "do nothing" group means a reduction in the size of user base. Based on the economic theory of clubs, Gopal and Sanders (1997) shows the reactions of piracy clubs to preventative controls. Too restrictive preventative controls make the pirates drop out of the club, which decreases the firm's profit.