An Analysis of Privacy-related Strategic Choices of Buyers and Sellers in e-Commerce Transactions

Spyros Kokolakis, Anastasopoulou Kalliopi, Maria Karyda
Dept. of Information and Communication Systems Eng.
University of the Aegean
Samos, Greece
{sak, k.anastasopoulou, mka}@aegean.gr

***Abstract*—E-commerce transactions, in addition to the exchange of goods and services for payment, often entail an indirect transaction, where personal data are exchanged for better services or lower prices. This paper analyses buyer's and seller's privacy-related strategic choices in e-commerce transactions through game theory. We demonstrate how game theory can explain why buyers mistrust internet privacy policies and relevant technologies (e.g. P3P) and sellers hesitate to invest in data protection.**

Keywords-information privacy; e-commerce; privacy economics; game theory

I. INTRODUCTION[1]

E-commerce applications collect buyers' personal data, either directly or indirectly. In some cases buyers have the option to refuse delivering information about them, as in the case when they are offered the option to register and create an account at an electronic shop, which they may refuse if they believe their privacy is at risk. If an electronic shop collects information indirectly, e.g. by means of recording buyers' online behavior, then buyers can use anonymity tools and techniques to conceal their identity.

On the other hand, electronic shops profit from personal data collection as they use them for reasons of marketing, pricing, and service improvement, or they simply sell them to third parties, though this is illegal in many countries, in particular in the European Union.

In any case, information about customers is valuable for electronic commerce enterprises and, thus, they use various means to make customers reveal personal information. The latter belong into two categories. First, there are incentives-based methods. They include price cuts, participation in contests and prize draws, personalized services, recommendations etc. Second, there are trust building methods, such as privacy policies and privacy seals.

An internet privacy policy is a statement that describes the ways a web site gathers, uses, discloses and manages a visitor's data. Although privacy policies are expected to promote trust in e-commerce, studies have shown that people rarely read and hardly ever understand privacy policies [1]. Other studies have shown that privacy policies tend to intensify privacy concerns instead of promoting trust [2].

Platform for Privacy Preferences (P3P) has been proposed to facilitate the use of online privacy policies. P3P is a protocol supported by the World Wide Web Consortium (W3C) that allows websites to state their intended use of information they collect about website users in a machine readable format [3]. P3P enabled the development of privacy agents (e.g. Privacy Bird[2] [4]) that can fetch P3P policies automatically, compare them with user's preferences, and alert and advice the user.

Privacy agents have been proven to be usable and to influence web users [5]. Nevertheless, neither P3P nor privacy agents have flourished. User adoption remains low [6] and online privacy policies are, in most cases, ignored by common users.

In this paper, we follow a game theoretic approach in an attempt to understand and analyze the low adoption of P3P, privacy agents, and relevant privacy enhancing technologies. We propose a model of buyer-seller interaction that regards privacy policies as the basis of an agreement between a buyer and a seller, where the seller declares to follow the provisions of the policy and the buyer is expected (though not obliged) to be honest in providing information.

In the following section we review the related work and in Section III we present our basic model. In Section IV we discuss the insights originating from our game theoretic model. The last section of the paper is devoted to conclusions and further research.

II. RELATED WORK

Game theory provides a strong analytical tool for the behavioral analysis of rational agents in many areas of social interaction, including privacy-related interaction.

Rajbhandari and Snekkenes [7] introduce game theory to privacy risk analysis. They substitute probabilistic estimation of events and consequences with the results of a game theoretic analysis. They present the case of a user that subscribes to a service from an online bookstore. In this case there are two players; the user and the online bookstore. The user can chose from two strategies, i.e. to provide genuine info or to provide fake info. Bookstore's strategies include

[1] This research has been co-financed by the European Union (European Social Fund - ESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF) - Research Funding Program: Heracleitus II. Investing in knowledge society through the European Social Fund.

[2] Privacy Bird ® is a registered trademark owned by AT&T Corp.

selling user's information to a third party or protecting it. The probabilities of each strategic choice are given by the mixed strategy Nash equilibrium and combined with the corresponding user's (negative) pay-offs they give a quantitative estimation of the level of privacy risk.

Friedman and Resnick [8] analyze the use of pseudonyms as a game of M players (where M >1). In this model users build online reputations based on pseudonyms and at each period of time they have the option to continue to play under their current identifiers or to get new ones. They show that this game is a repeated prisoner's dilemma type of game and results in suboptimal equilibria. To avoid suboptimality they suggest methods of limiting identity changes.

Taylor, Conitzer and Wagman [9] study the use of consumer data to exercise price discrimination. They analyze a model with a monopolist and a continuum of heterogeneous consumers, where consumers are able to maintain their anonymity and avoid being identified as past customers, possibly at a cost. They conclude that when consumers can costlessly maintain their anonymity, they all choose to do so, which paradoxically results in a higher profit for the firm.

Van Otterloo [10] studies the case of consumers that formulate their strategies considering the fact that the shop is watching their strategic choices. Thus, consumer's utility does not only depend on the value of the expected outcomes of strategic choices, but also on the information properties of the strategy chosen. They define two types of games, *the minimal information game* and *the most normal game* and show that in both games we can establish the existence of Nash equilibria.

Joshi, Sun and Vora [11] investigate the case of eBay-like auctions when a price-ascending auction is followed by a "second-chance offer", i.e. a price-discrimination stage. They develop a game theoretical model and examine two possibilities (i.e. to provide or not privacy protection against anonymity and bid secrecy) and the corresponding privacy cost.

Concluding, current research has applied game theory in some specific privacy-related topics and it has been shown that game theory can significantly contribute to our understanding of privacy-related behavior.

III. THE BASIC MODEL

Consider an electronic shop that offers prices not significantly different from those of similar e-shops. This e-shop collects personal information in order to offer personalized services and publishes a well structured (e.g. P3P-based) online privacy policy. A potential buyer examines the privacy policy and decides to proceed with a buy. Buyer and seller now have an agreement, though it might not be a legally binding one. The e-shop is expected to adhere to the declared privacy policy and the buyer is expected to provide valid information.

However, both have the option not to act as expected. The e-shop may sell customer information to a third party or use it in another profitable way that violates its privacy policy. The buyer, on the other hand, may provide false information. In this way, the buyer gets protected from privacy violations, but loses the benefits of personalized services.

Each player decides on a strategy based on his/her expectation of the other party's behavior. Thus, examining each party's behavior separately would not allow us to understand the dynamics of the buyer-seller interaction. This is a typical case where game theory constitutes an appropriate method of analysis.

The above buyer-seller interaction can be modeled as a game with both parties having two strategic options: to Cooperate (C) or to Defect (D). Cooperation for the seller means conforming with the privacy policy, whilst defecting means violating the policy. Respectively, cooperation for the buyer means to provide valid information, whilst defecting means faking personal information. So, there are four combinations (strategy profiles), which we present in the following paragraphs together with the corresponding payoffs.

If they both chose to defect, the buyer receives the minimum benefit, the one resulting from fulfilling the transaction. We arbitrary give it a value of one (1). In a similar manner the seller gets the minimum benefit resulting from selling the product, which we also give the value of one (1).

If the buyer defects, whilst the seller respects the privacy policy, then the buyer again gets the minimum benefit (1) and the seller will get the benefit of selling the product minus the cost of maintaining the privacy policy. Thus, we consider the payoff for the seller to be less than in the previous case, so we give it the value of zero (0).

If the buyer provides valid information and the seller mistreats it in some way, then the seller gets a significant profit and the buyer suffers a loss, assuming that we have a privacy-sensitive buyer. We consider a payoff of three (3) for the seller and (0) for the buyer.

Finally, both of them cooperate, then they will both benefit. The buyer will get personalized services and the seller may use buyer's data, within the limits of the privacy policy. We consider a payoff of two (2) for each of the players. The game in normal form is presented in Table I. Note that we use arbitrary values for the payoffs, for illustrative reasons. However, only the order of values is significant for the analysis that follows and not the exact values.

For the seller, defecting is a dominant strategy, since regardless of the buyer's choice seller gets a better payoff. So, we can eliminate the dominated strategy for seller (cooperate) and examine how the buyer would respond to the only remaining seller's strategy (defect).

TABLE I. THE BUYER-SELLER PRIVACY GAME

		Buyer	
		C	***D***
Seller	***C***	2,2	0,1
	D	3,0	1,1

TABLE II. EQUILIBRIA IN VARIATIONS OF THE BUYER-SELLER PRIVACY GAME

	One-off	Repeated	Infinitely repeated
Observable violation	D, D	D, D	C, C
Undetectable violation	D, D	D, D	D, D

In this case the buyer will also defect. Thus, the equilibrium in the above game (often called the *iterated dominant strategy equilibrium*) is {Defect, Defect}. You may note that in the equilibrium state the overall payoffs are less than when both players cooperate.

We have assumed that this game is played only once. However, a seller would normally expect the buyer to visit the e-shop again and make more transactions. So, if the game is repeated there are two more factors to take into consideration. First, whether there are finite or infinite repetitions and second whether seller's policy violation gets detected. If policy violation doesn't get detected then the iterative version of the game is identical to the one-off game presented above. So, we only examine the case of observable policy violation, i.e. one that gets immediately detected, e.g. spamming.

In the finite case the game is repeated several times and then stops. To find the solution for this game we should first examine the last round. We observe that the game played at the last round is identical to the one we presented above. Thus, the buyer would expect that the seller will violate the policy the last time the game it is played. However, for the buyer it would be too late to fake its information. So, if the buyer assumes that at some time in the future the seller will mistreat the information provided, then he/she will fake its information from the beginning. Thus, the equilibrium of the finite repeated game is the same as in the case of the one-off game.

When a customer remains loyal to e-shops that considers reliable and makes regular buys, we may model the relevant game as an infinitely repeated game, although it would eventually end at some time. The case of the infinitely repeated game is more complex. Since the buyer could stop buying from the particular e-shop (we don't consider monopolies) there is never a genuine infinitely repeated game. However, we can simplify our analysis, if we consider the act of discontinuing the buyer-seller relation as a penalty imposed by the buyer to the unreliable seller. The penalty is equivalent to the loss of profit from all future purchases. Whilst we leave the formal modeling and analysis of the game for future research, a rough analysis would show that respecting the privacy policy is a dominant strategy for the seller.

Concluding, the equilibria of the different variations of the buyer-seller privacy game are summarized in Table II.

IV. DISCUSSION

In the following paragraphs we shall attempt to interpret the results of the game theoretic analysis and discuss possible remedies.

The preceding analysis shows why it is difficult to establish trust with regard to the use of personal information in electronic commerce. Any e-shop that does not consider retaining its customers for a long period to be a desirable or attainable aim would choose to exploit the personal information of its customers in order to maximize its profit.

Thus, in an internet market where customers move from shop to shop without any migration cost and without any benefit from remaining loyal to a particular e-shop privacy policies can not establish trust. E-shops would not invest in establishing and maintaining a strict privacy policy. Since, consumers don't know in advance which e-shop is reliable and which is not, they will employ some privacy protection technique. In most cases they would fake their personal information.

On the contrary, e-shops targeting consumers that would make regular buys and remain loyal if satisfied would refrain from mistreating personal information of their customers. However, this holds only for observable policy violations.

If privacy policy violations have a low probability to get detected, then the privacy-sensitive consumer would assume that the e-shop will mistreat his/her personal information and, thus, he/she will employ some method of privacy protection.

Thus, since voluntary privacy policies and relevant technologies, such as P3P and Privacy Agents, are not able to establish trust between sellers and buyers, we should seek for remedies. Our analysis shows that any remedy should either address consumer loyalty or impose a penalty to violating sellers. Some options are:

- Regulate the use of policies by enforcing audits. However, one should consider the cost of audits and the possible low effectiveness, since such violations are notoriously difficult to detect.
- Impose high penalties for violating e-shops. However, this will only be effective if there is a reasonable detection rate.
- Establishing reputation systems. This is an effective strategy in several cases. If privacy violating sellers expect to lose massively potential buyers, then they might not risk mistreating the personal information of their customers.

In any case, the above conclusions only apply to privacy-sensitive buyers. We should not disregard the fact that a large part of the population is not willing to put much effort in protecting their privacy, either because they feel that the information they reveal in not very sensitive, or because they feel that in the Internet world there is no effective way to protect your privacy.

V. CONCLUSIONS AND FURTHER RESEARCH

This paper has developed and analyzed a game theoretic model to examine the inability of internet privacy policies to establish a trust relation between sellers and buyers. It was shown that although it would be more profitable for sellers and buyers to be honest to each other and cooperate, the buyer-seller game will end in an equilibrium where the seller does not abide to the privacy policy and the buyer provides

fake information. As a result, internet privacy policies are disregarded by consumers.

We have also shown that in order for privacy policies to have an impact on consumer they should be accompanied by regulations that impose a high penalty for violating sellers or reputation systems that increase the cost of violation.

Nevertheless, this study has several limitations as some potentially significant factors have been excluded. Specifically we have excluded the factor of discount of future benefits, which is a common factor in infinitely repeated games. We have only considered the game between a buyer and a seller and we have not analyzed the case of many buyers that communicate with each other and exchange information about the trustworthiness of sellers. Finally, we have not considered consumers that are not privacy sensitive.

In this paper we have not presented the formal definition and analysis of our game model, so as to make it readable for a wider audience. Formal definition and analysis is left for future research.

REFERENCES

[1] L.F. Cranor, "P3P: Making privacy policies more useful", *IEEE Security and Privacy,* vol. 1, no. 6, Nov.-Dec. 2003, pp. 50-55.

[2] I. Pollach, "What's wrong with online privacy policies?", *Communications of the ACM*, vol. 30, no. 5, Sep. 2007, pp. 103-108.

[3] W3C, "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification", Nov. 2006, available online at: http://www.w3.org/TR/P3P11/ (last access 04 May 2012).

[4] L.F. Cranor, P. Gudure, M. Arjula, "User interfaces for privacy agents", *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 13, June 2006, pp. 135-178.

[5] K.-P. L. Vu, V. Chambers, B. Creekmur, D. Cho, R. W. Proctor, "Influence of the Privacy Bird® user agent on user trust of different web sites", *Computers in Industry,* vol. 61, May 2010, pp. 311-317.

[6] P. Beatty, I. Reay, S. Dick, and J. Miller. "P3P Adoption on E-Commerce Web sites: A Survey and Analysis", *IEEE Internet Computing,* vol. 11, March 2007, pp. 65-71.

[7] L. Rajbhandari and E.A. Snekkenes, "Using Game Theory to Analyze Risk to Privacy: An Initial Insight", in Fischer-Hubner et al. (eds), Privacy and Identity 2010, IFIP AICT 352, 2001, pp. 41-51.

[8] E.J. Friedman and P. Resnick, "The Social Cost of Cheap Pseudonyms", *Jourrnal of Economics and Management Strategy*, vol. 10, no. 2, 2001, pp. 173-199.

[9] C.R. Taylor, V. Conitzer and L. Wagman, "Online Privacy and Price Discrimination", Economic Research Initiatives at Duke Working Paper No. 79, July 2010, Available at http://ssrn.com/abstract=1695143 (last accessed 04 May 2012).

[10] S. van Otterloo, "The value of privacy: optimal strategies for privacy minded agents", in Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems (AAMAS '05), ACM, 2005, pp.1015-1022.

[11] S. Joshi, Y.A. Sun, P. Vora, "Randomization as a strategy for sellers during price discrimination, and impact on bidders' privacy", in Proceedings of the 5th ACM workshop on Privacy in electronic society (WPES '06), Alexandria, Virginia, USA, Oct. 2006, pp. 73 – 76.