Privacy Decision-Making in the Digital Era: A game theoretic review

Callia Anastasopoulou[1], Spyros Kokolakis[1] and Panagiotis Andriotis[2]

[1]Dept. of Information and Communication Systems Engineering

University of the Aegean, Samos, Greece

[2] FET - Computer Science and Creative Technologies, University of West England (UWE), Bristol, U.K

{sak, k.anastasopoulou}@aegean.gr, Panagiotis.Andriotis@uwe.ac.uk

Abstract

Information privacy is constantly negotiated when people interact with enterprises and government agencies via the Internet. In this context all relevant stakeholders take privacy-related decisions. Individuals, either as consumers buying online products and services or citizens using e-government services, face decisions with regard to the use of online services, the disclosure of personal information, and the use of privacy enhancing technologies. Enterprises make decisions regarding their investments on policies and technologies for privacy protection. Governments also decide on privacy regulations, as well as on the development of e-government services that store and process citizens' personal information. Motivated by the aforementioned issues and challenges, we focus on aspects of privacy decision-making in the digital era and address issues of individuals' privacy behavior and issues of strategic privacy decision-making for online service providers and e-government service providers.

Keywords: Information Privacy, Decision-Making, Human Behavior, Strategic Interactions, Game Theory

1. Introduction

Information privacy is a multi-disciplinary and crucial topic for understanding the digital world (Regan, 2002; Acquisti, 2015). The information privacy usually relates to personal data stored on computer systems such as medical records, financial data, and business related information. Information privacy is also known as data privacy. In this research our interest focuses on online privacy where all personal data shared over the Internet.

adfa, p. 1, 2017.

Current research on information privacy highlight issues such as privacy concerns of online users (Tsai et al., 2011; Acquisti et.al, 2016), the privacy paradox between users' concerns and their privacy-related behaviors (Young and Quan-Haase, 2013; Liang et al.,2016), privacy-enhancing technologies (Parra-Arnau et al. 2015).

In the information age, privacy has become a luxury to maintain as data privacy can be violated on the internet through technical tools such as cookies or tracking online activities (Pan and Zinkhan, 2006; Aguirre et al., 2016). The rapid growth of the Internet and what it has brought to people's lives especially during the past ten years are truly astonishing. The internet makes people's lives incredibly convenient and websites will remain an important communication channel because the age of network information has really come.

Privacy however is not just an IT problem, although it could be in many cases. Many psychological, social and cultural factors play a significant role in the field of privacy. Human behavior is a considerable variable as individuals interact with others in online environments exchanging private information and making decision about their privacy. Privacy is a central regulatory human process by which individuals make themselves more or less accessible to others.

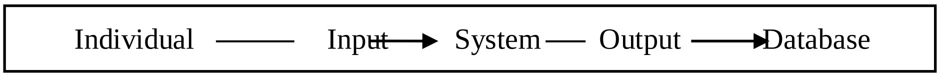

Fig.1: Describe the Information Flow

The variety of information that individual share online can be potentially characterizing them (Nosko et al., 2010; Alberts et al., 2015). The mechanisms that individuals use when making online sharing decisions are the main focus of this research.

The individual decision process with respect to privacy is affected by multiple factors. Incomplete information, bounded rationality, and systematic psychological deviations are considerable variables that influence individual's privacy sensitive behavior (Acquisti, 2004; Adjerid et al., 2016). First, incomplete information refers to privacy decision making where third parties share personal information about an individual without his being part of the transaction. Information asymmetries (how personal information will be used—might be known only to a subset of the parties making decisions), risk (most privacy related payoffs are not deterministic), and uncertainties (payoffs might not only be stochastic, but dependent on unknown random distributions). Benefits and costs associated with privacy intrusions and protection are complex, multifaceted, and context – specific. They are frequently bundled with other products and services (for example, a search engine query can prompt the desired result but can also give observers information about the searcher's interests), and they are often recognized only after privacy violations have taken place. They can be monetary but also immaterial and, thus, difficult to quantify.

Second, even if individuals had access to complete information, they would be unable to process and act optimally on vast amounts of data. Especially in the presence of complex, ramifying consequences associated with the protection or disclosure of personal information, our innate bounded rationality limits our ability to acquire, memorize and process all relevant inform action, and it makes us rely on simplified mental models, approximate strategies, and heuristics. These strategies replace theoretical quantitative approaches with qualitative evaluations and "inspirational" solutions that stop short of perfect (numerical) optimization.

Bounded problem solving is usually neither unreasonable nor irrational, and it needs not be inferior to rational utility maximization. However, even marginal deviations by several individuals from their optimal strategies can substantially impact the market outcome.

Third, even if individuals had access to complete information and could successfully calculate optimization strategies for their privacy-sensitive decisions, they might still deviate from the rational strategy. A vast body of economic and psychological literature has revealed several forms of systematic psychological deviations from rationality that affect individual decision making (Kahneman and Tversky, 2000 & 2016).For example, in addition to their cognitive and computational bounds, individuals are influenced by motivational limitations and misrepresentations of personal utility. Experiments have shown an idiosyncrasy between losses and gains (in general, losses are weighted heavier than gains of the same absolute value), and documented a diminishing sensitivity for higher absolute deviations from the status quo. Research in psychology also documents how individuals mispredict their own future preferences or draw inaccurate conclusions from past choices. In addition, individuals often suffer from self-control problems - in particular, the tendency to trade off costs and benefits in ways that damage their future utility in favor of immediate gratification. Individuals' behavior can also be guided by social preferences or norms, such as fairness or altruism. Many of these deviations apply naturally to privacy-sensitive scenarios. Any of these factors might influence decision-making behavior inside and outside the privacy domain, although not all factors need to always be present. Empirical evidence of their influence on privacy decision making would not necessarily imply that individuals act recklessly or make choices against their own best interest. It would, however, imply bias and limitations in the individual decision process that we should consider when designing privacy public policy and privacy -enhancing technologies.

2. Privacy Trade-offs in the Digital Age

What are the privacy implications of behavioral decision-making in Online Transactions? To answer this question we should notice what Privacy is for.

For decades a long-lasting debate exists between scholars to define exactly what that right entails (Post, 1991). Undoubtedly, privacy is a fundamental human right (Warren & Brandeis, 1890), but also a “chameleon” that changes meaning depending on context (Kang, 2012). Looking for a privacy definition in literature we found clear disarray. Nobody seems to have a very clear idea what the right to privacy is (Nofel et.al, 2014). Solove (2006) points out that Privacy means different things to different people.

Warren and Brandeis (1890) described Privacy as the protection of individuals’ space and their right to be left alone. Other authors have defined privacy as the control over personal information (Westin, 1967), or as an aspect of dignity, integrity and human freedom (Schoeman, 1992). Nonetheless, all approaches have something in common, a reference to the boundaries between private and public.

Privacy in the modern world has two dimensions: first, issues to do with the identity of a person and secondly, the way personal information is used. Individuals during their daily online transaction as consumers and rational agents have many topics to consider and decisions to make related to Privacy. Consumers seek for maximum benefits and minimum cost for themselves and for society. Firms on the other hand can benefit from the ability to learn so much about their customers. Under the above prism scientists working on behavioral decision-making research focus on the trade-offs and the protection or sharing of information (Acquisti et.al, 2015).

Privacy transactions nowadays occur in three different types of markets (Acquisti, 2010). First, transactions for non-privacy goods where consumers often reveal personal information, which may be collected, analyzed and processed someway. In this case, a potential secondary use of informati0n considered as a possible outcome. The second type of privacy-related transactions occurs where firms provide consumers free products or services (e.g. search engines, online social networks, free cloud services). In these transactions, consumers provide directly personal information, although the exchange of services for personal data is not always a visible. A third type of privacy-related transactions occurs in the market of privacy tools. For example, consumers may acquire a privacy enhancing technology to protect their transactions or hide their browsing behavior (Acquisti et.al, 2013).

Data exchange of consumers can improve firms' marketing capabilities, increase revenues through targeted offers and find innovative strategies in order to allure consumers to provide easily more personal information and shape preferences (Pitta, 2010). Observing consumers’ behavior, firms can learn how to improve their services and shoot at price discriminations strategies for clear profit (Acquisti & Varian, 2005). On the other hand, consumers benefit from targeted advertisement strategies, since advertisements are tailored to consumers' interests. Such targeting benefits both firms to reduce communication cost with consumers, and the consumers to gain easily useful information (Tucker, 2011).

Finally, a more intangible but also important form of indirect consumers' costs is related with the fact that the more an individual's data is shared with other parties, the more those parties gain a bargaining advantage in future transactions with that individual. While consumers receive offers for products, data holders accumulate data about them over time and across platforms and transaction. This data permits the creation of a detailed dossier of the consumers' preferences and tastes, and the prediction of her future behavior (Farrell, 2012).

Results from literature about privacy transactions show that decision-making for the collection and diffusion of private information by firms and other third parties will almost always raise issues for private life. Consumers seem to act shortsightedly when trade-offs apply short term benefits and long term costs for privacy invasions. This suggests that consumers may not always behave rationally when facing privacy trade-offs. Current research talks about the Privacy Paradox phenomenon where individuals face obstacles in making privacy sensitive decisions because of incomplete information, bounded access to the available information, and plenty deviations and behavioral biases suggested by behavioral decision research (Acquisti, 2004; Acquisti & Grossklags ,2007).

3. Human Aspects of Information Privacy in Cloud Computing: a game theory approach

In the literature the most studies of cloud computing adoption are conducted on which factors affecting the adoption of cloud computing in organization (Low et al., 2011; Morgan & Conboy, 2013 and Lian et al., 2014). However, cloud computing adoption by the organizations can be considered as a utopia, if individual users are not familiar with the new cloud technology. Sharma et.al (2016) point out studies from the field of information systems where behavioral constructs are key factors influencing individual user to adopt a new technology (Al-Somali, Gholami, & Clegg, 2009; Davis, 1989; Sharma and Govindaluri, 2014; Venkatesh et al., 2003). Sharma et. al. (2016) examines if and into what extent factors such as perceived usefulness, perceived ease of use, computer self-efficacy and trust can affect individual users to adopt cloud technologies and indicates that the above factors were found to be important indeed.

A major inhibiting factor has to do with the loss of control over storage of critical data and the service’s outsourced nature. The challenge for cloud providers is to identify and understand the concerns of privacy-sensitive stakeholders, and adopt security practices that meet their requirements (Brunette and Mogull, 2009). Misunderstanding the privacy concerns of end users may lead to loss of business, as they may either stop using a perceivably insecure or privacy-abusing service, or falsify their provided information –

hence minimizing the potential for profit via personalized adverting. An end user can give fake data if she believes that the service provider is going to abuse the privacy agreement and sell personal data derived from a cloud–based subscription to a third party.

Samarati and Vimercati (2016) underline that the significant benefit of elasticity in clouds appealed companies and individual users to adopt cloud technologies. At the same time this benefit is proved as harm for users' privacy as security threats and a potential loss of control of the owners of the data exists. In this case, the adoption and acceptance of the cloud computing paradigm is reduced. *ENISA (2009)* lists the topic of loss of control over data as a top risk for cloud computing. Also, in 2013 the "*Cloud Security Alliance - CSA"* lists data breaches and data loss as two of the top nine threats in cloud computing. The new complexity of the cloud paradigm (e.g. distribution and virtualization), the class of data (e.g. sensitive data) or the fact that CSPs might be not fully trustworthy are topics that increase security and privacy treats for cloud adoption.

Game theory in these cases emerges as an interesting tool to explore, as it can be used to interpret stakeholder interactions and interdependencies across the above scenarios. For example, Rajbhandari and Snekkenes (2011) implemented a game theory based approach to analyze risks to privacy, in place of the traditional probabilistic risk analysis (PRA). Their scenario is based on an online bookstore where the user has to subscribe in order to have access to a service. Two players take part in this game: the user and the online bookstore. The user could provide either genuine or fake information, whereas the bookstore could sell user's information to a third party or respect it. A mixed strategy Nash equilibrium was chosen for solving the game, with user's negative payoffs, in order to describe quantitatively the level of privacy risk.

Snekkenes (2013) applies Conflicting Incentives Risk Analysis (CIRA) in a case where a bank and a customer are involved in a deal. Snekkenes attempts to identify who is to take the role of the risk owner in case of data breach incidents and what are utility factors weighted on the risk owner's perception of utility. The CIRA approach identifies stakeholders, actions and pay-offs. Each action can be viewed as a strategy in a potentially complex game, where the implementation of the action amounts to the participation in a game. CIRA shows how this method can be used to identify privacy risks and human behavior.

Also, according to Hausken (2002), the behavioral dimension is a very important factor in order to estimate risk. A conflict behavior, which is recorded on individuals' choices, can be integrated in a probabilistic risk analysis and analyzed through game theory. Friedman and Resnick (2001) worked on providing the use of "cheap pseudonyms" as a way to measure reputation in Internet interaction between stakeholders. This was a game of M players where users provided pseudonyms during an interaction in the Internet world and they had the option either to continue playing with the current pseudonym or fin a new one, at each period of time. A suboptimal equilibria is found, as a repeated prisoner's dilemma type of game, while methods of limiting identity changes are suggested.

Cai et. al. (2016) inserts a game-theory approach to manage decision errors, as there is gap between strategic decisions and actual actions. They study the effects of decision errors on optimal equilibrium strategy of the firm and the user. Cavusoglu & Raghunathan (2008) propose game theory for determining if a provider should invest on high or low cost ICT and compare game theory and decision theory approaches. They show that in cases where firms choose their action, before attackers choose theirs (sequential game), firms gain the maximum payoff. Also, when firms adopt knowledge from previous hacker attacks and uses learns to estimate future hacker effort, then the distance between the results of decision theory and game theory approaches is diminishing.

Gao and Zhong (2016) address the problems of distorted incentives for stakeholders in an electronic environment, applying differential game theory in a case where two competing firms offer the same product to customers and the one can influence the value of their information assets by changing pricing rates. To assure consumers that they do not risk losing sensitive information, and also, increase consumer demand, firms usually integrate their security investment strategies. Researchers reveal that, higher consumer demand loss and higher targeted attacks, avert both firms from aggressive defense policy against hackers and would rather prefer to decrease the negative effect of hacker attacks by lowering their pricing rates.

Concluding, game theory research in online privacy-related decision-making has shown that it can give credible results in understanding privacy-related behavior.

4. Impact of Consumer Trust in Cloud Services

Sato (2010) refers that 88% of consumers, world-wide, are worried about loss of their data. Who has access to their data? Where consumers' data is physically stored? Can cloud service providers (CSPs) find ways to gain consumers' trust? Is the CSPs attempt towards consumer trust, a value for money strategy? These are typical questions that consumer and CSPs make about trust in clouds and online environments.

Ramachandran and Chang (2016) provide key issues associated with data security in the clouds. One key factor for cloud adoption is building trust when storing and computing sensitive data in the cloud Trust related to e-services offered in virtual online environments is a major topic for both consumers and cloud service providers, as well as for cloud researchers. Trust is strongly tied to online security. McKnight et.al (2002) indicate three significant trust components: *ability*, *integrity* and *good will* as prominent factors for a new ICT adoption. Ability is equal to CSPs efficiency in resources and skills that will not deter consumers from adopting cloud technologies. Integrity refers to CSPs obligations to comply with regulations and good will means that CSPs assure priority to consumers' needs.

Sharma (2016) suggests that trust in clouds has a positive and significant relationship with individual's decision to adopt cloud computing services. In clouds, users often want to share sensitive information and CSPs should ensure their privacy (King and Raja, 2012). Svantesson and Clarke (2010) suggested that CSPs apply such policy to ensure users that their data are safe and allure them to use clouds.

Consumers trust CSPs only to the extent that the risk is perceived to be low and the convenience payoff for them high. Pearson (2013) argues that when customers have to decide about trusting CSPs for personal data exchange services, they should consider organization's operational, security, privacy and compliance requirements and choose what best suit them.

5. Asymmetric Information and Strategic Stakeholders Interaction in Clouds

Asymmetric information is a concept encountered often in commercial transactions between sellers and buyers, end-users and service providers where the one party has more information compared to the other. Potentially, this could lead to a harmful situation as the one party can take advantage of the other party's lack of knowledge. Information asymmetries are commonly met in principal–agent problems where misinforming caused and the communication process is affected (Christozov et.al, 2009).

Principal–agent problems occur when an entity (or agent) makes decisions on behalf of another entity: the "principal – a person, who authorizes an agent to act with a third trusted-party"(Eisenhardt, 1989 and Bosse & Phillips, 2016). A dilemma exists when the agreement between participants is not respected and the agent is motivated to act in his own personal gain and in contrary to the "principal". Principals do not know enough about whether an agreement has been satisfied and therefore their decisions are taken under some risk and uncertainty and involve costs for both parties. The above information problem can be solved if the third trusted-party provides incentives so as the agents to act appropriately and in accordance with the principals. In terms of game theory, rules should be changed so that the rational agents confronted with what principal desires (Bosse & Phillips, 2016).

McKinney and Yoos (2010) refers that information is almost always unspecified to an unbounded variety of problems and the involved agents (so-called stakeholders) almost always act without having full information about their decisions. Whilst literature on information risk is adequately studied in the last decades, there is no risk premium for information asymmetry (Hirshleifer et.al, 2016). Easley and O'Hara (2004) argue that information asymmetry creates something called information risk and their model showed that more private information from consumers receives higher expected returns to the involved agents.

For an agent, a risk premium is the minimum economic benefit by which the expected return from a decision- making under risk must exceed the known return on a risk-free decision where full information is provided to the involved stakeholders. It is positive if an agent is risk averse, namely when he exposed to uncertainty caused by information asymmetry, to attempt to reduce that uncertainty. The utility of such a strategic movement expected to be high in many cases. For such risky outcomes, a decision-maker adopts a criterion as a rule of choice, where higher expected value strategic movements are simply the preferred ones (O'Brien and Ahmed, 2016).

From a game theory perspective, uncertain outcomes exist potential preferences with regards to appropriate risky choices coincide. In cases where the above expected utility hypothesis is satisfied, it can be proved useful to explain choices that seem to contradict the expected value criterion. Asymmetric information in clouding introduces scenarios where stakeholders (consumers and service providers) interact strategically. A game theory approach based on trust is regarded as a useful tool to explain the conflict and cooperation between intelligent rational decision-makers.

Public clouds considered as a great advantage for stakeholders in terms of flexibility, scalability and cost effectiveness. Despite the advantages, the feature of public clouds subject to security issues and challenges according to data control, which still remain unresolved. Njilla et. al (2016) introduce a game theoretic modeling for trust in clouds suggesting that risk and trust are two behavioral factors that influence decision-making in uncertain environments like cloud markets where consumers seem not to have full control over their stored data. They adopt a game theoretic approach to establishing a relationship between trust and factors that could affect the assessments to risk. The scenario refers to three players: end-users, service providers, and attackers. Provider defends the system's infrastructure against attackers, while end-users tempt not to trust an online service in case of data privacy breaches. Njilla et. al. (2016) propose a game model which mitigate cyber attack behavior in security implementation. They analyze different solutions obtained from the Nash equilibrium (NE) and find that frequent attacks with contemporary providers' ability to mitigate the loss, might cause the attacker to be detected and caught. Thus, it is possible in that case attacker not attack because of high risk and penalties. But what about the gain and the loss when the provider invests in security and the attacker decides to attack and succeeds his target with users' private data compromised? What are the payoffs of each player in this case? This regarded as an open question.

Maghrabi and Pfluegel (2015) use game theory by an end-user perspective to assess risk since moving to public clouds. While previous works focus on how to help cloud provider to assess risk, they develop a model for benefits and costs associated to attacks on the end-user's asset in order to help user to decide whether or not adopt the cloud. The end-user is conformed to a Service Level Agreement (SLA), which promises to protect against external attacks. The writers suggest that they can use the degree of trust T that a user have in cloud provider. Pure Nash equilibrium exists for values T = 0 and T = 1 and Maghrabi and Pfluegel compute a mixed Nash equilibrium in case where T is between 0 and 1. The above user-centric game model using the notion of trust results to a pure Nash equilibrium for completely trusted cloud provider and for complete lack of trust in the provider.

Douss et al. (2014) propose a game trust model for mobile ad hoc networks. Assuring reputation and establishing trust between collaborating parties is indirectly a way to provide secure online environment. The authors suggest an evaluation model for trust value. They applied computational methods and developed a framework for trust establishment.

Li et.al. (2016) study price bidding strategies when multiple users interact and compete for resource usage in cloud computing. The provided cloud services are available to end-users with a pay-as-you-go manner (Kaur and Chana, 2014; Pal and Hui, 2013). A non-cooperative game model is developed with multiple cloud users, where each cloud user has incomplete and asymmetric information about the other users. They work on utility functions with the "time efficiency" parameters incorporated to calculate net profit for each user, in order to help them to decide whether to use the cloud service. For a cloud provider, the income is the amount of money users pay for resource usage (Mei et.al., 2015). A rational user will maximize his net reward by choosing the appropriate bidding strategy $(=U_{\text{of choosing the cloud service}} - P_{\text{ayment}})$. However, it is irrational for a cloud provider to provide enough resources for all potential requests in a specific time. Therefore, cloud users compete for resource usage. The above stakeholders' strategic interactions are analyzed from a game theoretic perspective and the existence of Nash equilibrium is also confirmed by a proposed near-equilibrium price bidding algorithm. For future research, a good idea is to study the cloud users' choice among different cloud providers or determine a proper mixed bidding strategy.

Fagnani et.al. (2016) consider a network of units (e.g smartphones or tablets) where users have decided to make an external back up for their data and also, are able to offer space to store data of other connected units. They propose a peer-to-peer storage game model and design also, an algorithm which makes units interact and store data back up from connected neighbors. The algorithm has been converged to Nash equilibrium of the game, but several challenges arisen for future research analysis related to stakeholders interactions in a more trusted environment.

Moreover, the resource allocation problem in cloud computing where users compete for gaining more space to run their applications and store their data is analyzed by Jebalia et.al. (2015). They develop a resource allocation model based on a cooperative game approach, where cloud providers provide a great number of resources in order to maximize profit and combine the adoption of security mechanisms with payoffs maximizing.

Security and privacy are often located as opposite concepts. Much of focus is on reducing cost during the establishment of a trust-worthiness infrastructure in cloud computing, which gradually requires disclosing private information and proposing a model of trading privacy for trust (Seigneur and Jensen, 2004; Njilla et al., 2016). Also, Lilien et al. (2008) indicate the difference between maintaining a high level of privacy and establishing trust for transactions in cloud environments. Users, who display a particular interest in concealing private information intensively, request from cloud providers a set of corresponding credentials which establishing trust for these users. The tradeoff problem exists where the assurance for the minimum user's privacy loss meet the choice of revealing the minimum number of credentials for satisfying trust requirements.

Raya et al. (2010) suggest a trust–privacy tradeoff game theoretic model that gives incentives to stakeholders to build trust and at the same time assure privacy loss at a minimum level. Individual players do not trust cloud providers unless they received an appropriate incentive.

Gal-Oz et al. (2011) introduce a tradeoff approach studying the relationship between trust and privacy in online transactions. They suggest that pseudonyms constitute a necessary component for maintaining privacy since pseudonyms prevent association with transaction ID and ensure a level of reputation. The more pseudonyms used, the more reputation is succeeded.

Following major problems has been observed during the study we indicate that any application relying upon an emerging cloud computing technology should consider the different possible threats. The problem is a lack of a clearly defined meaning of such a risk that benefits the cloud users to make proper choice and cloud service providers to avoid threats efficiently.

6. Conclusions and future research

A game theory approach is adopted as a very general language for modeling choices by agents in whom the actions of other agents can affect each player's outcome. Game theory assumes players choose strategies which maximizes utility of game outcomes given their beliefs about what others will do.

The most challenging question is often how beliefs are formed. Most approaches suggest that beliefs derived from what other players are likely to do. In equilibrium, beliefs about others assume to be correct which answer the question of how to specify reasonable beliefs by equating choices.

However, some limits are arisen. First, many games that occur in social life are so complex , which means that at a specific time players cannot form accurate beliefs what other players would choose and therefore they cannot choose equilibrium strategies. So, what strategies might be chosen by players with bounded rationality, or when there is learning from a repeated game? Second, in empirical works, only received payoffs are easily measured (e.g. prices in auctions). A huge variety of experiments show that game theory sometimes explains behavior adequately, and sometimes is badly rejected by behavioral and process date (Camerer, 2003). The above inference can be used to create a more general theory which matches the standard theory when it is accurate, and can explain the cases in which is badly rejected. This emerging approach is called "behavioral game theory" which uses the analytical game theory to explain observed violations by incorporating bounds on rationality.

Game theory is the standard theory to analyze cases where individuals or firms interact, for example, strategic interaction of privacy-sensitive end-users use of cloud based mobile apps, e-commerce transactions between sellers and consumers, and many other social dilemmas such as the provision of public goods. Behavioral game theory introduces psychological parameters which amplify a rational scenario and give a motivational basis for players' behavior. Representation, social preferences over outcomes, initial conditions and learning are the basic components for a precise analysis (Camerer, 2003).

In this work we focus on Information Privacy in Cyberspace Transactions. Cyberspace is a synopsis for the web of consumer electronics, computers, and communication networks that interconnects the world. The potential surveillance of electronic-activities presents a serious threat to information privacy. The collection and use of private information have caused serious concerns about privacy invasion by consumers, creating a personalization–privacy tradeoff. The key approach to address privacy concerns is via the protection of privacy through the implementation of fair information practices, a set of standards governing the collection and use of personal information. We take a game-theoretic approach to explore the motivation of firms for privacy protection and its impact on competition and social welfare in the context of product and price personalization. We find that privacy protection can work as a competition-mitigating mechanism by generating asymmetry in the consumer segments to which firms offer personalization, enhancing the profit extraction abilities of the firms. In equilibrium, both symmetric and asymmetric choices of privacy protection by the firms can result, depending on the size of the personalization scope and the investment cost of protection. Further, as consumers become more concerned about their privacy, it is more likely that all firms adopt privacy protection. In the perspective of welfare, we show that autonomous choices of privacy protection by personalizing firms can improve social welfare at the expense of consumer welfare. We further find that regulation enforcing the implementation of fair information practices can be efficient from the social welfare perspective mainly by limiting the incentives of the firms to exploit the competition-mitigation effect.

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. We 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.

Another reference and up-to-date research field is related with privacy concerns in Cloud Computing. Free mobile applications of cloud computing offer a range of diverse services (e.g. gaming, storage etc.) usually in return for delivering personalized advertising to their consenting end-users. In order to do so they may retain a range of personal information such as location and personal preferences. Thus, privacy-related interactions between service providers and end users are important to be studied as personal data are valuable in a subscription-based cloud system. In our research a game theory approach is used as a tool to identify and analyze such interactions in order to understand stakeholder choices, as well as how to improve the quality of the service offered in a cloud computing setting.

References

Acquisti, A. (2004).“Privacy in Electronic Commerce and the Economics of Immediate Gratification,” Proc. ACM Conf. Electronic Commerce (E 04), ACM Press, pp.21–29.

Acquisti, A. and J. Grossklags (2007). What can behavioral economics teach us about privacy? In S. G. C. L. Alessandro Acquisti, Sabrina De Capitani di Vimercati (Ed.), Digital Privacy: Theory, Technologies and Practices, pp. 363–377. Auerbach Publications (Taylor and Francis Group).

Acquisti, A. (2010). The economics of personal data and the economics of privacy. Background Paper for OECD Joint WPISP-WPIE Roundtable.

Acquisti, A., L. K. John, and G. Loewenstein (2013). What is privacy worth? The Journal of Legal Studies, Vol.42, No. 2, pp.249-274

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). “Privacy and human behavior in the age of information”. Science, Vol.347, No. 6221, pp.509-514.

Acquisti, A., Taylor, C. R., and Wagman, L. (2016). The economics of privacy. Available at SSRN 2580411.

Acquisti, A. and H. R. Varian (2005). Conditioning prices on purchase history. Marketing Science 24 (3), 367{381.

Adjerid, I., Peer, E., & Acquisti, A. (2016). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. Available at SSRN 2765097.

Aguirre, E., Roggeveen, A. L., Grewal, D., and Wetzels, M. (2016). The personalization-privacy paradox: implications for new media. Journal of Consumer Marketing,Vol.33, No.2, pp.98-110.

Alberts, J. K., Nakayama, T. K., & Martin, J. N. (2015). Human communication in society. Pearson.

Al-Somali, S. A., Gholami, R., and Clegg, B. (2009). An investigation into the acceptance of online banking in Saudi Arabia.Technovation, 29(2), 130-141.

Bosse, D. A., and Phillips, R. A. (2016). Agency theory and bounded self-interest. Academy of Management Review, 41(2), 276-297

Brunette, G. and R. Mogull (ed). 2009. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance, December 2009.

Cai, C. X., Mei, S. E., and Zhong, W. J. (2016). A game-theory approach to manage decision errors. In MATEC Web of Conferences (Vol. 44). EDP Sciences.

Camerer, C.F. (2003). *Behavioral Game Theory: Experiments on Strategic Interaction. Princeton, NJ:Princeton University Press.*

Christozov, D., Chukova, S., and Mateev, P. (2009). Informing processes, risks, evaluation of the risk of misinforming. Foundations of informing science, pp. 323-356.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, Vol. 13 No. 3, pp. 319-339.

Cavusoglu, H., Raghunathan, S., and Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. Journal of Management Information Systems, 25(2),pp.281-304.

Douss, A. B. C., Abassi, R., and El Fatmi, S. G. (2014, September). A Trust Management Based Security Mechanism against Collusion Attacks in a MANET Environment. In Availability, Reliability and Security (ARES), 2014 Ninth International Conference on (pp. 325-332). IEEE.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. Academy of management review, 14(1), 57-74.

European Network and Information Security Agency – ENISA (2009). Cloud Computing: Benefits, Risks and Recommendations for Information Security. Available at: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (accessed 14/07/2016).

Fagnani, F., Franci, B., and Grasso, E. (2016). A game theoretic approach to a peer-to-peer cloud storage model. arXiv preprint arXiv:1607.02371.

Farrell, J. (2012). The economics of privacy: Can privacy be just another good? J. onTelecomm. and High Tech. L., Vol.10, pp.251-445.

Gao, X., and Zhong, W. (2016). A differential game approach to security investment and information sharing in a competitive environment. IIE Transactions, 48(6), 511-526.

Gal-Oz, N., Grinshpoun, T., and Gudes, E. (2011). Privacy issues with sharing reputation across virtual communities. In Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society (p. 3). ACM.

Hausken K. 2002. "Probabilistic risk analysis and game theory Risk Analysis", vol. 22, pp. 17–27.

Hirshleifer, D. A., Huang, C., and Teoh, S. H. (2016). Information Asymmetry, Market Participation, and Asset Prices. Market Participation, and Asset Prices.

Jebalia, M., Ben Letaïfa, A., Hamdi, M., and Tabbane, S. (2015). An overview on coalitional game-theoretic approaches for resource allocation in cloud computing architectures. International Journal of Cloud Computing 22, 4(1), 63-77.

Kahneman D. and Tversky A., Choices, Values, and Frames, Cambridge Univ. Press, 2000.

Kang, J., Shilton, K., Estrin, D., Burke, J. and Hansen, M. (2010)."Self-Surveillance Privacy" Iowa Law Review, Vol. 97, p. 809, 2012; UCLA School of Law Research Paper No. 11-01. Available at SSRN: http://ssrn.com/abstract=1729332 or http://dx.doi.org/10.2139/ssrn.1729332

Kaur, P. D., and Chana, I. (2014). A resource elasticity framework for QoS-aware execution of cloud applications. Future Generation Computer Systems, 37, 14-25.

Liang, H., Shen, F., and Fu, K. W. (2016). Privacy protection and self-disclosure across societies: A study of global Twitter users. Available at New Media and Society, 1461444816642210.

Lian, J. W., Yen, D. C., and Wang, Y. T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital.International Journal of Information Management, 34(1), p.p.28-36.

Lilien, L., and Bhargava, B. (2008). Trading privacy for trust in online interactions. Idea Group.

Low, C., Chen, Y., and Wu, M. (2011). Understanding the determinants of cloud computing adoption.Industrial ManagementandData Systems, 111(7), p.p.1006-1023

Li, W., and Huang, Z. (2016). The Research of Influence Factors of Online Behavioral Advertising Avoidance. American Journal of Industrial and Business Management, 6(09), 947.

Maghrabi, L., and Pfluegel, E. (2015). Moving assets to the cloud: A game theoretic approach based on trust. In Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on (pp. 1-5). IEEE.

McKnight, D.H., Choudhury, V. and Kacmar, C., (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building mode. *Journal of Strategic Information Systems 11* (3-4), pp.297–323.

McKinney Jr, E. H., and Yoos, C. J. (2010). Information about information: A taxonomy of views. MIS quarterly, pp.329-344.

Mei, J., Li, K., Ouyang, A., and Li, K. (2015). A profit maximization scheme with guaranteed quality of service in cloud computing. IEEE Transactions on Computers, 64(11), 3064-3078.

Morgan, L., and Conboy, K. (2013). Key factors impacting cloud computing adoption. Computer, 10,97e99

Mullainathan,S., and Thaler, R.H.2001. Behavioral Economics International Encyclopedia od Social Sciences, 1st edn, pp.1094-1100.Pergamon.

Njilla, L. Y., Pissinou, N., and Makki, K. (2016). Game theoretic modeling of security and trust relationship in cyberspace. International Journal of Communication Systems, 29(9), 1500-1512.

Nofer, M., Hinz, O., Muntermann, J., and Rossnagel, H. (2014). "The Economic Impact of Privacy Violations and Security Breaches," Business and Information Systems Engineering: Vol. 6: Iss. 6, 339-348

Nosko, A., Wood, E., and Molema, S. (2010). All about me: Disclosure in online social networking proles: The case of FACEBOOK. Computers in Human Behavior, Vol.26, No.3, pp.406-418, ISSN 07475632.

O’Brien, M. K., and Ahmed, A. A. (2016). Rationality in human movement. Exercise and sport sciences reviews, 44(1), 20-28.

Pal, R., and Hui, P. (2013). Economic models for cloud service markets: Pricing and capacity planning. Theoretical Computer Science, 496, 113-124.

Pan, Y., and Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. Journal of Retailing, Vol.82, No.4, pp.331-338.

Parra-Arnau, J., Rebollo-Monedero, D., & Forné, J. (2014). Measuring the privacy of user profiles in personalized information systems. Future Generation Computer Systems, 33, 53-63.

Pearson, S. (2013). Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing (pp. 3-42). Springer London.

Pitta, D. (2010). Jump on the bandwagon{its the last one: New developments in online promotion. Journal of Consumer Marketing 27 (2).

Post, R. C.(1991). "Rereading Warren and Brandeis: Privacy, Property, and Appropriation", Case Western Reserve Law Review: Vol41, Article 3.

Rajbhandari, L. and Snekkenes, A. "Mapping between Classical Risk Management and Game Theoretical Approaches", Lecture Notes in Computer Science, Springer, 2011, pp. 147-154 (Vol.7025) Doi: 10.1007/978-3-642-24712-5_12

Ramachandran, M., and Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. International Journal of Information Management, 36(4), 618-625.

Regan, P. M. (2002). Privacy as a common good in the digital world. Information, Communication and Society, 5(3), 382-405.

Raya, M., Shokri, R., and Hubaux, J. P. (2010, March). On the tradeoff between trust and privacy in wireless ad hoc networks. In Proceedings of the third ACM conference on Wireless network security (pp. 75-80). ACM.

Samarati, P., and di Vimercati, S. D. C. (2016). Cloud security: Issues and concerns. Wiley, New York.

Sato, M. (2010). Personal data in the cloud: A global survey of consumer attitudes. Minato-ku, Tokyo 105-7123, JAPAN

Gao, X., and Zhong, W. (2016). A differential game approach to security investment and information sharing in a competitive environment. IIE Transactions, 48(6), 511-526.

Schoeman, F. D. (1992). Privacy and social freedom. Cambridge university press.

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., and Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. Computers in Human Behavior, 62, pp.61-69.

Sharma, S. K., and Govindaluri, S. M. (2014). Internet banking adoption in India: structural equation modeling approach. Journal of Indian Business Research, 6(2), 155-169

Seigneur, J. M., and Jensen, C. D. (2004). Trading privacy for trust. In International Conference on Trust Management (pp. 93-107). Vol.2995 Springer Berlin Heidelberg.

Snekkenes, E. (2013). Position Paper: Privacy Risk Analysis Is about Understanding Conflicting Incentives. In IFIP Working Conference on Policies and Research in Identity Management (pp. 100-103). Springer Berlin Heidelberg.

Solove, D. J. (2006). “A taxonomy of privacy”. University of Pennsylvania Law Review 154 (3), 477.

Svantesson, D. and Clarke, R. (2010) Privacy and consumer risks in cloud computing *Computer law and security review*,26 (4), pp.391-397.

Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research, 22(2), 254-268.

Tucker, C. (2011b). Social Networks, Personalized Advertising, and Privacy Controls. Mimeo, MIT.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User acceptance of information technology: toward a unified view.MIS Quarterly, 425-478.

Young, A. L., and Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. Information, Communication and Society, 16(4), 479-500.

Warren, S. D., and Brandeis, L. D. (1890). The right to privacy. In Harvard Law Review vol. 4, pp. 193–220.

Westin A. (1967) Privacy and Freedom. New York: Atheneum, ISBN0370013255, 9780370013251.