The role of perceived privacy and perceived security in online market

R. Mekovec*and Ž. Hutinski*
*University of Zagreb, Faculty of organization and informatics, Varaždin, Croatia
renata.mekovec@foi.hr and zeljko.hutinski@foi.hr

Abstract - Individuals mostly hesitate to use services offered via Internet due to their suspicions regarding the level of offered (1) protection of their privacy and (2) security of performing online transactions. Privacy is mostly concerned with the identifiable user data and users' rights to have control over their data. On the other hand, security provides the physical, logical, and procedural safeguards that are needed to keep the data private. Privacy cannot be achieved without obtaining security practice, nor will the usage of security mechanisms guarantee protection of privacy. Despite being closely linked in practice, privacy and security are perceived as separate issues by online users. Therefore, in this article the relationship between various privacy factors (factors that influence users' privacy concerns) and the perception of security protection during users' online activities is discussed. The role that perceived privacy and perceived security have in the e-service users' evaluation of a service is investigated.

I. Introduction

In the past decade we have witnessed extensive growth of electronic commerce. Internet has become a key communication media between companies and their customers. Accordingly, various web services provide "support" for individuals' daily activities, e.g. online shopping, e-banking or for communication with the government, doctors or professors (using e-government, e-health or e-learning services). Hence, more and more data about individuals' online behaviour are being collected. This causes concerns over the security of the transaction (and collected data) as well as concerns over the privacy protection of the individuals. Eurostat's data [1] shows that 35% of respondents (included in research in 2010) do not use online services due to their concerns regarding security of transactions, and 30% of respondents do not use online services due to issues related to privacy concerns, e.g. loss of personal data.

Thus, in order to increase the online users' confidence in the security of their data, companies (online service providers) should have various mechanisms that control access to the stored data [2]. On the other hand, the risk of online users' loss of control over their personal information should be reduced. Online users should have control (1) over disclosure of their personal information to others, as well as (2) over future usage of the disclosed information [3].

This article is focused on online users' perception of privacy and perception of security during their online activities. The research was performed to measure concerns of online shopping and e-banking users regarding their privacy perception. Various privacy factors were included to measure online users' overall privacy concerns. Perception of security was also measured. Relationship between perceived privacy and perceived security was investigated. In addition, the relationship between perceived privacy and security on one hand, and perceived quality of e-service on the other hand, was examined.

There are several important reasons to investigate online users' perception of privacy and security issues: (1) technology has great impact on privacy by making it easy to digitalise information, so it is easy to collect and search for information about anybody, (2) digitalised information usually cannot be deleted so every individuals' activity in the digital world exists in perpetuity, (3) there is evident growth of online users' awareness of their lack of privacy protection and possibility of their privacy invasion.

Online users are more and more familiar with Internet usage, as well as with their privacy rights. The role of information security is to implement the mechanisms that will grant one's rights to privacy [4]. Accordingly, online users' awareness of possible security mechanisms is rising. Therefore, they can define their requirements regarding the privacy and security protection. In addition, this can result in their resistance to use an e-service from a service provider which doesn't meet their needs. Online service with the best (lowest) price isn't always a good ground for the service provider to build competence. Online users will include various issues in an evaluation of a service and overall service quality, as well as benefits that they will gain.

II. Online privacy and security

As the Internet is becoming a crucial part of people's lives, more companies use the Internet for business. This resulted with the transmission of large amounts of data where the capacity for storing, retrieving and monitoring data evidently rises. Obviously, Internet has two different faces [5]. One enables exciting opportunities for individuals to work, network and spread their ideas online. The other makes people vulnerable and prevents them from participating equally in online environment.

Online users' behaviour is influenced by the trade-offs between what one gives up (like disclosure of some kind of information) and what one gains from it (benefits like 24/7 availability of service, time-saving or other conveniences). Meanwhile, increased risk in online scenarios is now recognized in a wide range of threats that seek to specifically target online users and exploit information about them.

Several studies suggest that Internet users have serious privacy and security concerns, and that their trust has the primary role in growth of e-commerce. Reference [6] has investigated the importance of four trust indices which influence Internet users purchase intention and willingness to provide personal information. The included trust indices were: (1) third party privacy seal, (2) privacy statement, (3) third party security seal, and (4) security features. The results indicate that respondents value security features the most.

Reference [7] investigated how perceived credibility influences the users acceptance of e-banking. Perceived credibility encompassed two dimensions: security and privacy concerns. Security referred to a level of assurance that a particular transaction will be performed without any security breach. Privacy referred to protection from the collection of various data during users' interaction with a bank. Results of the performed investigation indicate that perceived credibility (e.g. to conclude that transactions are secured and are protecting their privacy) had a significant positive effect on users' behaviour intentions. Authors in [8] identified sixteen e-business risks. In the study participants were asked to rate their perceptions of 16 risks. Three top concerns for 200 included participants were profitability risk, security risk and privacy risk. The relationships between three trust considerations (vendor, Internet and third parties) and customers' attitudes towards online purchasing were examined [9]. The authors found that the relationship between trust in a vendor and attitude towards online purchasing becomes more important when people have higher privacy and security concerns. In addition, they found that when people have higher privacy and security concerns the relationship between trust in Internet and attitude towards online purchasing weakens.

Managing risk related to e-business is an important issue. The lessons to be learnt include identifying e-business risks and using appropriate mechanisms to manage them. The study presented in this article is focused on risks identified as critical – privacy and security risks.

A. Online privacy

Privacy can be seen as a boundary control process where an individual defines with whom he will communicate and what type of communication (and how much) will occur [10]. Boundary control enables the particular individual to achieve the desired level of contact with others, at a particular time and according to stated conditions. Two types of factors have an impact on the process of boundary control: (1) situational factors and (2) personal factors. Situational factors encompass social and physical elements. Social elements refer to the existence of others with whom the individual can communicate, others' characteristics, and willingness to communicate. Physical elements refer to physical barriers, location and distance. Personal factors are related to individuals' characteristics, like their need for privacy.

Online privacy is accordingly defined as an exchange of Internet users' personal information for some benefits [11]. On the other hand, the term online privacy is usually connected with information privacy and therefore is described as Internet users' concerns regarding their ability to control the collection of their personal information, as well as to control the future usage of the collected information or the information that were generated based on their online activities [12].

According to their concerns regarding information privacy individuals can be grouped in three groups [13]: (1) privacy guardians, (2) information sellers and (3) convenience seekers. Privacy guardians are individuals who are very concerned about their information privacy. Information sellers are individuals who will trade their personal information for a small award. Finally, convenience seekers are individuals who are primarily focused on benefits that can be gained from the disclosure of their personal information.

The information about online users collected during their online activities can be arranged in three groups [14]: (1) anonymous information (e.g. information about IP address of the computer that has been used, type of web browser), (2) personally non-identifying information (e.g. information about age, gender, education, interests) and (3) personally identifying information (e.g. name, e-mail address, postal address, telephone number, credit card number).

Online privacy data can be categorized according to operations performed on data [15]: (1) data collection and (2) data use. Data collection process can be divided in four categories: (1) volunteered data collection for public use, (2) volunteered data collection for private use, (3) un-volunteered but noticed data collection, and (4) un-volunteered but unnoticed data collection. In category volunteered data collection for public use following data can be distinguished: (1) online registration data, (2) online administrative data, and (3) online facilitation data. On the other hand, volunteered data collection for private use includes (1) online survey data (e.g. online market survey, opinion research) and (2) online purchaser data (e.g. age, gender, credit card number, e-mail address). Category un-volunteered but noticed data collection includes online transaction data collected via interactive online shopping or online mail catalogue. During un-volunteered but unnoticed data collection click-streams data on Internet usage are collected. Data use process includes the following data operations: marketing, data disclosure to third parties and data sale to third parties.

B. *Online security*

First step of privacy related management is the identification and classification of data that need to be protected. When it is known what should be protected, the next question is how should it be protected. Information security can be defined as a discipline that uses the concepts of confidentiality, integrity, and availability to answer the question of how data should be protected. This CIA triad is enforced using various protective mechanisms like encryption, authentication, intrusion detection and etc. Questions that should be answered when dealing with the protection of information security are [16]:

1. Are the data protected from being disclosed to individuals that should not access them?
2. Are the data protected from being created, changed or deleted by individuals that do not have permission for these activities?
3. Are the data available to those who need them?

If a company cannot maintain the security of the data that it has collected from its customers through online channels, then it is evident that the company isn't meeting the demanded level of corporate responsibility [17].

Online users are increasingly finding themselves exposed to security risks during their online activities. Security risks include the threats like manipulation with information and/or networks (e.g. destruction, selling or modification of data) or various types of fraud and misuse [18]. Perceived online security is defined as online users' perception of how they are protected from risks related to security. Reference [19] used the term Perceived Security Protection (PSP) to describe consumers' perception that the Internet vendor will fulfil security requirements (such as authentication, integrity, and encryption).

Two main factors concerning perceived security in e-commerce can be distinguished [20]: (1) perceived operational factor and (2) perceived policy-related factor.

Perceived operational factor includes actions that a website can take to ensure that the users feel secure during the online interaction. On one hand, perceived operational factor includes: the site's blocking of unauthorized access; emphasis on login name and password authentication; funding and budget spent on security; monitoring of user compliance with security procedures; integration of state-of-the-art systems; distribution of security items within the site; website's encryption strategy; and consolidation with network security vendors. On the other hand, perceived policy-related factor includes the following items: the website's emphasis on network security; top management commitment; effort to make users aware of security procedures; the website's keeping up-to-date with product standards; the website's emphasis on security in file transfers; and issues concerning the web browser.

III. RESEARCH

The research was performed in order to investigate the level of Internet users' perception of online privacy and overall e-service quality. In addition, Internet users' perception of online security was measured. Finally, the relationship between perceived privacy, perceived security and perceived service quality was examined.

A. *Respondents*

Included participants were individuals who had been using online shopping and e-banking service (for at least a year). The research included 185 respondents of whom 63% were men and 37 % were female.

B. *Measurement and results*

Fourteen privacy factors were included in the investigation of Internet users' privacy perception. Privacy factors are factors that influence the overall perception of privacy in online environment. Detailed overview, systematisation and categorisation of proposed privacy factors, as well as a detailed research model of online shopping/e-banking users' privacy perception was reported elsewhere [21].

Research was performed using a written and an online questionnaire. Questionnaire consisted of 94 items. Respondents were using five-point Likert scale (5 = strongly agree, 1 = strongly disagree) to mark their agreement or disagreement with a particular item. Privacy factors included in research were labelled as follows: Control over information collection – CIC, Control over information usage – CUI, General information sensitivity – ISG (in general, during daily online activities), Legislation and government privacy protection – LPG, Service e-tailer's reputation – STR, Personal Internet interest – PII, Control – COL, Improper access – IA, Information sensitivity – ISS (when using online shop or bank service), Perceived Internet privacy risks – PIPR, Unauthorised secondary usage – USU, Perceived credibility – PC, Perceived integrity – PI, and Perceived benevolence - PB.

Perceived security (PS) was measured using five-item scale (items PS1-PS5). Security perceived by respondents referred to their judgment regarding security of transaction and security of collected data when using online shopping and e-banking service. Descriptive statistics regarding the items used to measure perceived security are presented in Table I. According to the presented results it can be concluded that perceived security is quite high with average score 4.01 (mean). Respondents are satisfied with security provided by online company or bank (whose service they were using). Minimum (average) score is marked for item PS2 (3.83) which is related with respondents' estimation if the data are secured during their usage of online shopping and e-banking service. Maximum (average) score is marked for item PS3 (4.14). This item is connected with respondents' judgment regarding the confidentiality of online transaction (online shopping and e-banking transaction).

TABLE I. DESCRIPTIVE STATISTICS FOR SCALE PERCEIVED SECURITY AND PERCEIVED PRIVACY

	Minimum	Maximum	Mean	Standard deviation	Variance
PS1 – security of transactions	2	5	4.11	0.675	0.456
PS2 – security of data	1	5	3.83	0.820	0.673
PS3 – transaction are confidential	2	5	4.14	0.822	0.676
PS4 – awareness of usage of security measures	1	5	4.07	0.828	0.685
PS5 – security of data transfer	1	5	3.92	0.820	0.673
Average perceived security	2.20	5.00	4.01	0.631	0.399
GPBC1 – uncertainty regarding paying with credit card online	1	5	3.44	1.127	1.269
GPBC2 – uncertainty regarding shopping online	1	5	3.24	1.263	1.595
GPBC3 – insecurity regarding privacy of data	1	5	3.21	1.207	1.458
GPBC4 – data privacy protection	1	5	3.69	1.137	1.292
Average perceived privacy	1.00	5.00	3.39	0.984	0.969

Overall online privacy perception (GPBC) was measured using four-item scale. Overall online privacy perception referred to online shopping and e-banking service users' anxiety about how an online company or bank (which is providing the e-service) will handle information that they collect about users during their online interaction. Results of the research shows that overall online privacy perception is 3.39 (mean). On proposed five-point scale this result is placed in the middle of the scale. This is a neutral result, neither are respondents concerned nor are they satisfied with the ways how information about them are handled by online companies or banks (whose service they used).

Overall service quality (PQual) was measured using two-item scale.

In order to explore relationships between perceived quality of service, perceived security and perceived privacy (and privacy factors) a correlation analysis was performed using Pearson coefficient. Table II. presents the results of the performed analysis (N=185, *p<0.05, **p<0.01).

Figure 1. illustrates the correlation between perceived privacy, perceived security and perceived service quality. In addition, the correlation between privacy factors and perceived (1) privacy, (2) security and (3) service quality are presented (where correlation coefficient is equal or greater than 0.350).

Perceived security is negatively correlated with perceived privacy (r= -0.182, p<0.05) and positively correlated with perceived service quality (r= 0.430, p<0.01). Respondents who perceived higher level of provided security were less concerned about their privacy protection. In addition, respondents who perceived higher level of security were also more satisfied with the quality of a provided service.

TABLE II. RESULTS OF CORRELATION ANALYSIS, n=185, ** p<0.01, * p<0.05

	PS	GPBC	PQual
CIC	-0.160*	0.352**	-0.129
CUI	0.207**	0.020	0.064
ISG	-0.141	0.443**	-0.179*
LPG	-0.059	0.210**	-0.138
STR	0.183*	0.139	0.145*
PII	0.045	0.064	-0.019
COL	-0.035	0.339**	-0.192**
IA	0.101	0.149*	0.026
ISS	-0.043	0.400**	-0.126
PIPR	-0.185*	0.363**	-0.140
USU	0.209**	0.064	0.044
PC	0.683**	-0.117	0.348**
PI	0.620**	-0.077	0.366**
PB	0.531**	0.009	0.243**
PS	1	-0.182*	0.430**
GPBC	-0.182*	1	-.290**
PQaul	0.430**	-0.290**	1

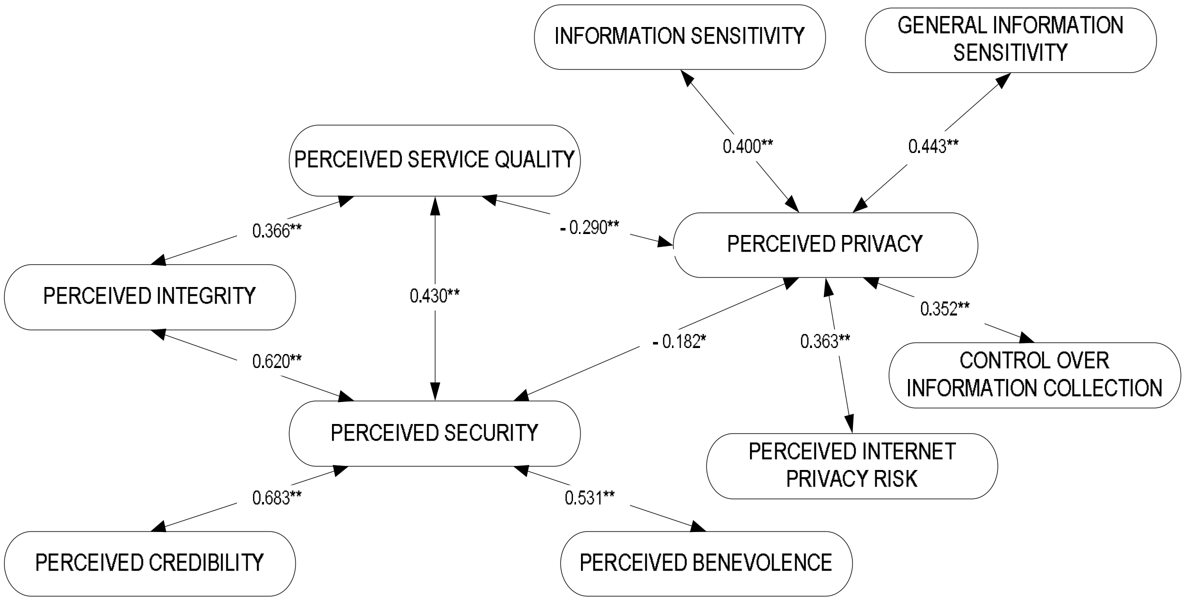

Figure 1. Correlation between (1) perceived service quality, (2) perceived security, (3) preceived privacy, and (4) privacy factors, n=185, ** p<0.01, * p<0.05

Further on, there is a negative correlation between perceived privacy and perceived quality (r= -0.290, p<0.01). Respondents who were less concerned about privacy protection perceived higher level of service quality.

Regarding the correlations between proposed privacy factors and perceived security the results of the correlation analysis indicate as follows. There is a significant correlation between perceived security and: (1) Control over information collection – CIC (r= -0.160, p<0.05), (2) Control over usage of information – CUI (r= 0.207, p<0.01), (3) Service e-tailer's reputation – STR (r= 0.183, p<0.05), (4) Perceived Internet privacy risk – PIPR (r= -0.185, p<0.05), (5) Unauthorized secondary usage – USU (r= 0.209, p<0.01), (6) Perceived credibility – PC (r= 0.683, p<0.01), (7) Perceived integrity – PI (r= 0.620, p<0.01), and (8) Perceived benevolence – PB (r= 0.531, p<0.01)

There is a significant correlation between perceived service quality and: (1) General information sensitivity – ISG (r= -0.179, p<0.05), (2) Service e-tailer reputation – STR (r=0.145, p<0.05), (3) Control – COL (r= -0.192, p<0.01), (4) Perceived credibility – PC (r= 0.348, p<0.01), (5) Perceived integrity – PI (r= 0.366, p<0.01), and (6) Perceived benevolence – PB (r= 0.243, p<0.01).

IV. Conclusion

Perception of privacy and perception of security are factors that affect costumers' trust in electronic commerce. Therefore companies that offer and sell their products or services online should put more efforts to positively influence costumers' perceptions of privacy and security [22]. Computer system security is a global problem that is affecting private as well as corporate users of information technology. Information technology users should be informed and should take responsibility for the security of resources that they are using. Accordingly, they should play an active role in protecting their privacy (in the use of computer or in the use of Internet) [23].

From a practical standpoint, the results highlight several issues that may guide the successful completion in electronic market. Specifically, we identified a significant relationship between perceived security and perceived privacy. If the online users are more convinced that a particular web site provides security of transaction and data they will be less concerned about their privacy protection. The relationship between (1) perceived security and (2) perceived privacy on one hand, and overall e-service quality (on the other hand) was confirmed. When online users are more satisfied with security protection they will be more satisfied with overall service quality. If online users are less concerned about their privacy protection, they will be more satisfied with overall service quality.

References

[1] Eurostat, Data in focus, 46/2009, Internet usage in 2009 - Households and Individuals, 2010, <http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-09-046/EN/KS-QA-09-046-EN.PDF>, (accessed on January 25, 2012)

[2] X. Ye, and L. Zhong, "Improving web service security and privacy," World Congress on Services, SERVICES 2011, Washington, DC, USA, July 4-9, 2011, IEEE Computer Society pp. 406–413.

[3] H-H. Hann, K-L. Hui, S-Y.T. Lee, I.P.L .Png, "Analyzing online information privacy concerns: an information processing theory

approach," Proceedings of the 40th Annual Hawaii International Conference on System Sciences, Hawaii, 3-6. January 2007.

[4] S. DeKay, K. Belva, "Privacy roles and responsibilities," in Enterprise information security and privacy, edited by C.W. Axelrod, J.L. Bayuk, D. Schutzer, Artech House, 2009, pp. 3-20.

[5] D.K. Citron, "Civil rights in our information age," in The offensive Internet edited by S. Levmore and M.C. Nussbaum, Harvard University Press, 2010, pp. 31-49.

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

[7] Y-S. Wang, Y-M. Wang, H-H. Lin, T-I. Tang, "Determinants of user acceptance of Internet banking: a empirical study," International Journal of Service Industry Management, vol. 14, 2003, pp. 501-519.

[8] J.E. Scott, "Measuring dimensions of perceived e-business risks," Information Systems and e-Business Management, vol. 2, 2004, pp. 31-55.

[9] P. McCole, E. Ramsey, J. Williams, "Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns," Journal of Business Research, vol. 63, 2010, pp. 1018–1024.

[10] D.M Pedersen, "Model for types of privacy by privacy functions, " Journal of Environmental Psychology, vol. 19, 1999, pp. 397-405.

[11] L. Ashworth, C. Free, "Marketing dataveillance and digital privacy: using theories of justice to understand customer's online privacy concerns," Journal of Business Ethics, no. 67, 2006, pp. 107-23.

[12] J.A. Castañeda, F.J. Montoro, "The effect of Internet general privacy concern on customer behavior," Electronic Commerce Research, vol 7, 2007, pp. 117-41.

[13] Ibid [3]

[14] R.K. Chellappa, R.G. Sin, "Personalization versus privacy: an empirical examination of the online consumer dilemma," Information Technology and Management, vol. 6, 2005, pp. 181-202.

[15] O.A.J. Mascarenhas, R. Kesavan, M.D. Bernacchi, "Co-managing online privacy: a call for joint ownership," Journal of Consumer Marketing, vol. 20, 2003, pp. 686-702.

[16] Ibid [4]

[17] O. Eisen, "Online security – a new strategic approach," Network security, July 2010, pp. 14-15.

[18] N.K. Malhotra, S.S. Kim, J. Agarwal, "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model," Information System Research, vol. 15, No. 4, 2004, pp. 336-55.

[19] D.J. Kim, D.L. Ferrin, H.R. Rao, "A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents," Decision Support Systems vol. 44, 2008, pp. 544–564.

[20] M.M. Yenisey, A.A. Ozok, G. Salvendy, "Perceived security determinants in e-commerce among Turkish university students," Behaviour & Information Technology, vol. 24, July 2005, pp. 259-274.

[21] R. Mekovec, "Online privacy: overview and preliminary research," Journal of Information and Organizational Sciences, vol. 34, 2010, pp. 195-209.

[22] R.K. Chellappa, "Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security," under submission, <http://www.bus.emory.edu/ram/ Papers/sec-priv.pdf>, (accessed on January 25, 2012)

[23] G. Bubaš, T. Orehovački, M. Konecki, "Factors and predictors of online security and privacy behavior," Journal of Information and Organizational Sciences, vol. 32, 2008, pp. 79-98.