Influence of the Perception of Data Security on Customer Usage of Internet Services

Erik Massarczyk, Peter Winzer
Faculty of Design – Computer Science – Media
RheinMain University of Applied Sciences
Wiesbaden, Germany
Email: erik.massarczyk@hs-rm.de, peter.winzer@hs-rm.de

***Abstract*—An increasing customer usage of Internet services with various devices demands a greater effort on data security and privacy issues, because more and more devices are connected and personal data are spread more widely. However, in many cases the performance of services is more important than the provision of data security. So, this leads to a need to investigate how the user perception of data security influences the usage of Internet services, which will be analyzed with the Technology Acceptance Model. Here, the aim of this paper is to figure out a possible negative impact of the perception of data security on the usage of Internet services. The aim of this paper will be that within the usage of the Technology Acceptance Model an influence of data security issues can be proven.**

Keywords-data security; devices; customer usage; Internet services.

I. INTRODUCTION

During the last 10 to 15 years, more and more people use the Internet and Internet services in their daily life. This development leads to a rising global Internet penetration and data flow [1]. Further, most people use mainly services for Social Media, broadcasting/streaming, gaming and cloud computing. Especially during the last years, people start to use the different services with various devices. This approach conducts that people apply more and more different devices for the usage of services [2][3]. Due to this application of services the devices get connected among each other. Hence, it can be assumed, that the personal user data spread to a larger degree [2]. For the customers of Internet services, it is elusive where the personal data is stored and who gets access to the personal data, because the smart connected devices cover wide range of information over geographical boundaries [3][4]. Finally, the usage of Internet services by customers faces the problem of data security and privacy from the user perspective. Personal data include critical information and intellectual properties about the users themselves and these data are countable assets from which enterprises, companies and also criminals can benefit [5].

In general, the users are responsible which personal data they spread for the usage of different Internet services. Hurdle free communication, marketing measures and advertisement disclose also more personal data of the users. Further, a lot of people are also willing to share their personal data in ignorance of risks of data leakage and data theft. Out of it, it can be concluded that data security and privacy gets more and more important, because more personal data is disclosed and often the users are not able to examine who gets access to their personal information and who uses them for legal and illegal motives.

The authors will figure out what the user perception of data security and privacy is, when they use different Internet services with various devices, especially mobile devices with wireless Internet connections. Moreover, each Internet usage is in direct connection with data security and privacy issues. For these reasons, it has to be investigated whether a higher perception of data security and trust in a service leads to a preferred usage of this service or device.

Accordingly, the authors analyze what the users of Internet services do to prevent unauthorized access to their personal data. In Section II, the term data security will be described. Following this section, the authors will figure out the challenges of service and technology usage. In Section IV, the methodology presents the theoretical background of our research and in Section V the further approach will be described.

II. DATA SECURITY

Data security conducts that users want to keep their personal data to themselves. Here, for the user must be clear, who gets access to the personal information. Hence, no one should get access to the user's personal data, who does not have the right permission for the usage [4]. However, a lot of companies use personal data of customers, which customers spread in their Internet services, because a lot of users are not fully aware of the possible risks of sharing information [5][6]. Furthermore, they do not know which huge amount of data they produce and how they can prevent such risks [7]. This behavior could be a problem for residential users, because 56% of Internet services and platforms transmit personal information without permissions to third parties [8]. So, users should be better informed and aware of their personal data. In many cases, persons divulge information, which they may regret in a future situation. Further, the data can be linked to critical personal information like credit card numbers, etc. [5][6].

In general, most users fear: (a) capturing of passwords and accounts, (b) blackmails, (c) eavesdropping, and (d) undesired access to personal data from criminals [2]. The users want a secure transmission of data and the services

 ISBN: 978-1-61208-502-9

should guarantee integrity, availability and confidentiality of the data and their transmission [9].

Otherwise, the users also have to prevent unauthorized accesses by changing the passwords regularly, what the authors also investigate with a survey. If the users lose their access and their data is leaked, normally the users have to bear the loss in reputation of image, business partners, relatives and friends [2].

III. CHALLENGES

The main challenge for analyzing user perceptions of data security is that all user attitudes and beliefs are completely subjective and depend on demographic (age) and cultural factors, which influence the customer willing to share data [5]. These discrepancies also include that each user has his perceptions of risks and prevention of risks. As mentioned in Section I, in many cases the people prefer to look for the performance of services instead of the security and data protection measures. To increase the customer caution for disclosure and leakage of private data, services should insert several measures and rules which the customers have to imply to use the services [10]. Further, services and applications should state consequences of misuse and data leakage and insert different messages to make sure that the users understand of their data distribution. However, it is necessary to investigate, what kind of impact the factors have on the individual perception of data security and the influence on the usage of Internet services, especially mobile services.

IV. METHODOLOGY

For the analysis of the connection between the perception of data security and the usage of Internet services, the authors will use the Technology Acceptance Model (TAM). The TAM shall clarify, how the customer individual's acceptance of Information Technologies (IT) can be explained and predicted [11][12]. Our paper will focus on the dependence of the usage of mobile Internet services on security issues and the acceptance of new technologies. It is currently known that the perceived usefulness has a positive impact on behavioral intentions, which turns in an actual customer usage [12]. However, perceived usefulness does not cover the user's perception, that the usage of the service will enhance his performance [11].

Moreover, perceived usefulness and behavioral intentions are not able to analyze and to reflect user perceptions of data security and the adoption of mobile Internet services. Therefore, the authors implement an external variable as influence factor for perceived usefulness. The external variable will be perceived credibility, which covers the user beliefs and attitudes that the used systems would be free of privacy and security threats [13]. Lin et al. further figured out that data security and privacy are the most affecting factors for an adoption of technology [13]. It is also known that perceived credibility influence positively the behavioral intention to use [14]. But, the authors do not conclude that users believe that using mobile Internet services will not imply security or privacy threats [14]. Here, the authors are of the opinion that the customers carry security and privacy threats by using mobile Internet services. To examine this hypothesis, the authors will use a survey to prove that data security issues have a negative impact on behavioral intentions to use mobile Internet services. For the analysis of the individual customer groups, separate cross-sectional surveys ("one-shot survey") will be conducted within a short period of time [15]. Here, the answers are taken by interviewers in personal oral interviews, thus ensuring completeness and accuracy of the answers. The personal interview will be conducted on the basis of a random quota sample based on the demographic characteristics of gender and age in order to be representative of the local population [16][17]. To cover the frequency of mobile data usage and the perception of data security, a 5-point-Likert-scale (very often to very few and very important to very important) will be implemented. The discrepancy to the previous study will be underlined by the analysis of other impact factors like culture values and traditions.

V. APPROACH

The idea of this paper is to present a relationship between a perception of data security and usage of Internet services, especially of mobile Internet services. After a review of literature to gain an overview about existing concepts and theories over customer behaviors in circumstances of data security issues, a survey shall find out and investigate current customer Internet behaviors. The data will be analyzed with quantitative research methods under usage of the statistical program Statistical Package for the Social Sciences (SPSS). After the evaluation credibility, the Exploratory Factor Analysis will be done to ensure the validity and to present related groups of perceptions and services. The analysis of the survey shall present the regression between the external variable perceived credibility and perceived usefulness and behavioral intentions. After completion of the data analysis, next steps aim at figuring out the results of least square regression and completion to support the hypothesis and findings of the TAM in relation of data security issues.

REFERENCES

[1] International Telecommunication Union (ITU), "ICT Facts & Figures – The world in 2015", May 2015, [Online]. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf, 2016.07.11.

[2] P. W. Dowd and J. T. McHenry, "Network Security: It's Time to Take It Seriously" Computer (1998), vol. 31, issue 9, IEEE, Sept. 1998, pp. 24-28.

[3] D. Desai, "Law and Technology – Beyond Location: Data Security in the 21st Century" Magazine Communications of the ACM (2013), vol. 56, issue 1, ACM, Jan. 2013, pp. 34-36.

[4] F. S. Ferraz and C. A. Guimarães Ferraz, "Smart City Security Issues: Depicting information security issues in the role of a urban environment", 7th International Conference on

Utility and Cloud Computing, IEEE/ACM, 2014, pp. 842-846.

[5] S. Dhawan, K. Singh, and S. Goel, "Impact of Privacy Attitude. Concern and Awareness on Use of Online Social Networking" 5th International Conference - Confluence The Next Generation Information Technology Summit 2013, IEEE, Sept. 2014, pp. 14-17.

[6] D. Malandrino, V. Scarano, and R. Spinelli, "How increased awareness can impact attitudes and behaviors toward online privacy protection", International Conference on Social Computing (Social Com), IEEE, Sept. 2013, pp. 57-62.

[7] A. N. Joinson. U.-D. Reips, T. Buchanan, and C. B. Paine Schofield, "Privacy, Trust, and Self-Disclosure Online", Human-Computer Interaction, vol. 25, no. 1, 2010, pp. 1-24.

[8] B. Krishnamurthy, K. Naryshkin, and C. Wills, "Privacy leakage vs. protection measures: the growing disconnect", in Web 2.0 Security and Privacy Workshop, 2011, pp. 1-10.

[9] D. Nayak, N. Rajendran, D. B. Phatak, and V. P. Gulati, "Security Issues in Mobile Data Networks" Vehicular Technology Conference (VTC 2004), vol. 5, IEEE , Sept. 2004, pp. 3229-3233.

[10] Q. Tan and F. Pivot, "Big Data Privacy: Changing Perception of Privacy, International Conference on Smart City/SocialCom/SustainCom, IEEE, 2015, pp. 860-865

[11] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, Vol. 13, 1989, pp. 318-340.

[12] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: a comparison of two theoretical models", Management Science, Vol. 35, 1989, pp. 982-1003.

[13] F.-T. Lin, H.-Y. Wu, and T. T. Nguyet Nga, "Adoption of Internet Banking: An Empirical Study in Vietnam", 10th International Conference on e-Business Engnineering, IEEE, 2013, pp. 282-287.

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

[15] A. Diekmann, „Empirical Social Research", [German] „Empirische Sozialforschung", Reinbek / Hamburg, Rowohlt-Taschenbuch-Verlag, Vol. 5, 2011

[16] J. Bortz and N. Döring, „Research Methods and Evaluations", [German] „Forschungsmethoden und Evaluation; für Human- und Sozialwissenschaftler", Heidelberg, Springer-Medizin-Verlag, vol. 4, 2009

[17] M. Kaya, „Data Collection Procedure", [German] „Verfahren der Datenerhebung", in Albers, S./Klapper, D./Konradt, U./Walter, A./Wolf, J. (Hrsg.): *Methodik der empirischen Forschung*, Wiesbaden, Gabler, vol. 3, 2013, pp. 49-64.

 ISBN: 978-1-61208-502-9