QUT

Queensland University of Technology
Brisbane Australia

This is the author's version of a work that was submitted/accepted for publication in the following source:

Lebek, Benedikt, Degirmenci, Kenan, & Breitner, Michael H.
(2013)
Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. In
19th Americas Conference on Information Systems (AMCIS 2013), 15-17
August 2013, Chicago, Illinois.

This file was downloaded from: https://eprints.qut.edu.au/105686/

http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/8/

Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices

Completed Research Paper

Benedikt Lebek
Leibniz Universität Hannover
Institute for Information Systems Research
lebek@iwi.uni-hannover.de

Kenan Degirmenci
Leibniz Universität Hannover
Institute for Information Systems Research
degirmenci@iwi.uni-hannover.de

Michael H. Breitner
Leibniz Universität Hannover
Institute for Information Systems Research
breitner@iwi.uni-hannover.de

ABSTRACT

The concept of Bring-Your-Own-Device (BYOD) describes the trend of employees using their private mobile devices to manage corporate data from anywhere at any time. BYOD can increase employees' productivity and be cost-cutting for organizations. To implement BYOD, organizations are dependent on employees' acceptance of BYOD, because employees' participation usually is voluntary. As employees' acceptance is affected by uncertainty, we investigate the influence of security, privacy, and legal concerns on the intention to use BYOD mobile devices. A research model is developed based on the theory of reasoned action (TRA) and the technology acceptance model (TAM), which is tested by means of structural equation modeling (SEM) with data collected from 151 employees. Our results indicate a significant impact of the concerns on employees' acceptance. Moreover, our study reveals employees' indecision towards their intention to use their private mobile devices for working purposes. Several implications for future research and practitioners are given.

Keywords

Bring-Your-Own-Device (BYOD), mobile devices, security concerns, privacy concerns, legal concerns, theory of reasoned action (TRA), technology acceptance model (TAM), structural equation modeling (SEM)

INTRODUCTION

As a result of innovations in the form and usability of mobile devices and the widespread adoption of mobile data networks (Tu and Yuan, 2012), mobile computing devices became a part of daily life for many users (Moreno, Tizon and Preda, 2012). Mobility is also a main driving factor of the modern service society (Zaplata, Lammersdorf and Kunze, 2009). Due to the increased convenience, efficiency, and productivity of mobile devices, more and more organizations are looking for ways to implement mobile devices into their information technology (IT) infrastructure to take advantage of the flexibility these devices offer (Scheepers and Scheepers, 2004).

At the intersection between private ownership and corporate deployment, the concept of bring-your-own-device (BYOD), emerged over the past several years and is already common in organizations of all sizes (Johnson and Joshi, 2012; Miller, Voas and Hurlburt, 2012). BYOD can be described as the use of employees' privately owned mobile devices for working purposes (Johnson and Joshi, 2012; Niehaves, Köffer and Ortbach, 2012), e.g. to "access corporate applications like email and databases; and to create, store and manage corporate data using these devices" (Osterman Research, 2012). Following Friedman and Hoffman (2008), mobile devices are "portable electronic systems that store and manipulate potentially confidential information". In the context of this study, we refer to smartphones and tablet PCs as mobile devices.

BYOD is often linked to several advantages for both employees and organizations. From an employees' point of view these are greater freedom and flexibility, increased motivation as well as easier adoption of technology (Niehaves et al., 2012). These benefits lead to a higher job satisfaction (Osterman Research, 2012). Since a positive job satisfaction increases

employees' productivity (Saari and Judge, 2004), organizations can also benefit from BYOD (Osterman Research, 2012; Dell and Intel Corp.[1], 2012). Furthermore, the use of BYOD mobile devices increases employees' availability and thus the flexibility and mobility of workforce when business needs occur. As a result, employees can work from home or on the move, so that business continuity does not suffer. Organizations can cut their IT costs as employees invest in their own mobile working devices (Dell and Intel Corp.[1], 2012; Niehaves et al, 2012; Osterman Research, 2012). These benefits provide an incentive for organizations to implement a BYOD strategy.

A precondition for a successful BYOD implementation is employees' acceptance, because an implementation usually depends on employees' voluntary participation. However, BYOD creates a "unique set of challenges for IT professionals" (Johnson and Joshi, 2012) as it "redefines the relationship between employees and the IT organization" (Niehaves et al., 2012). Following Oliver and Bearden (1985), we argue that employees' acceptance is not only dependent on employees' perceived benefits, but is also impacted by employees' perceived concerns. In practice, concerns regarding security, privacy, and legal aspects of BYOD are discussed (e.g. Miller et al., 2012; Osterman Research, 2012; Silvergate and Salner, 2011).

Although these concerns are common in the context of end users' acceptance of mobile services (e.g. Giessmann, Stanoevska-Slabeva and de Visser, 2012), the examination of concerns in the context of BYOD has been considered little in IS research literature (Niehaves et al., 2012). To the best of our knowledge, there is no research investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. For this reason, we intend to fill this research gap with our study and aim to answer the following research question:

> RQ: *To which degree do security, privacy, and legal concerns affect employees' intention to use BYOD mobile devices?*

A research model is developed to explain the influence of perceived concerns and perceived benefits on employees' attitude towards BYOD and their intention to use BYOD mobile devices. The research model is based on the theory of reasoned action (TRA) and the technology acceptance model (TAM) and is derived from validated previous studies.

The paper is structured as follows: First, we give a theoretical background and generate hypotheses before the data collection process and the research methodology are described. Then, the results of the study are discussed and theoretical contributions as well as practical implications are worked out. Finally, limitations of the study are noted and directions for future research are given.

THEORETICAL BACKGROUND AND HYPOTHESES

As the purpose of this study is to examine the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices, it is important to explain employees' intention in the first place. Intention has been employed as the key dependent variable to describe user acceptance of IT in numerous studies (e.g. Davis, 1989; Nysveen, Pedersen and Thorbjørnsen, 2005; Taylor and Todd, 1995; Venkatesh and Davis, 1996). Ajzen (1991) defines intention as an indication "of how hard people are willing to try, of how much of an effort they are planning to exert, in order to perform the behavior". In the context of this study, the behavior is the actual usage of BYOD mobile devices. According to the theory of reasoned action (TRA) (Fishbein and Ajzen, 1975) the most immediate antecedent of intention is attitude, which is defined as „an individual's positive or negative feelings (evaluative affect) about performing the target behavior" (Davis, Bagozzi and Warshaw, 1989). Thus, we propose the following hypothesis:

> H1:   *Attitude will have a significant positive effect on the intention to use BYOD mobile devices.*

Attitude relates to beliefs about consequences of behavior and the evaluation of those consequences (Fishbein and Ajzen, 1975). In view of beliefs, Oliver and Bearden (1985) distinguish between benefits and problems, which both are associated with the behavior.

With regard to benefits in the context of IT at the workplace, Davis (1989) indicates that people are motivated to use a system that helps them perform their jobs. He explains that "people are generally reinforced for good performances by raises, promotions, bonuses, and other rewards." These benefits are indicated as perceived usefulness, which is defined as „the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989). The technology acceptance model (TAM) (Davis et al., 1989) postulates that perceived usefulness affects attitude due to positively or negatively valued outcomes. In addition, it is hypothesized that perceived usefulness has a direct influence on intention, because „within organizational settings, people form intentions toward behaviors they believe will increase their

---

[1] http://content.dell.com/us/en/corp/d/corp-comm/the-evolving-workforce

job performance, over and above whatever positive or negative feelings may be evoked toward the behavior per se" (Davis et al., 1989). In this context, the word useful means "capable of being used advantageously" (Davis, 1989).

According to several studies, the concept of BYOD entails advantages for both employees and organizations. For example, a recent study by Dell and Intel Corp.[2] revealed that granting employees more privileges towards a more mobile workplace increases the overall productivity within an organization. Moreover, by allowing employees to choose their mobile working devices, their individual efficiency could be enhanced. A study by Osterman Research (2012) revealed similar results concerning employees' productivity and efficiency. The study explains the gain in employees' productivity and efficiency by a higher job satisfaction. This is the result of an increased personal freedom since employees can use their preferred mobile devices in their favored locations and time. According to this, from an organizational point of view, BYOD can be beneficial, as it reduces corporate costs since employees fund their own mobile devices.

In view of problems within the frame of organizational IT, the construct of uncertainty has been in the focus of several studies (e.g. Harnesk and Lindström, 2011; Spears and Barki, 2010). Uncertainty can be defined as „the degree to which the future states of the environment cannot be accurately anticipated or predicted due to imperfect information" (Pavlou, Liang and Xue, 2007). Considering the usage of BYOD mobile devices, we define perceived usefulness as perceived benefits and problems as perceived uncertainty and adapt these constructs to our research model.

> *H2:*   *Perceived benefits will have a significant positive effect on (a) attitude and (b) intention to use BYOD mobile devices.*

> *H3:*   *Perceived uncertainty will have a significant negative effect on the attitude towards BYOD.*

Pavlou et al. (2007) propose that perceived uncertainty is influenced by security concerns and privacy concerns. In the context of BYOD, legal concerns are considered to be a third factor influencing uncertainty (Miller et al., 2012; Osterman Research, 2012; Silvergate and Salner, 2011).

Security concerns can be defined as „the level to which an employee believes that her/his organizational information assets are threatened" (Herath and Rao, 2009). In academic literature, there is consent that the implementation of mobile technology into organizations entails information security concerns (e.g. Beulen and Streng, 2002; Giessmann et al., 2012; Scheepers and Scheepers, 2004). With the use of BYOD mobile devices, corporate information security is exposed to new risks (Niehaves et al., 2012; Tu and Yuan, 2012). Employees are often unaware of their responsibilities regarding the security of corporate information assets. For example, private cloud services are often used to store corporate data leaving data integrity and confidentiality at risk (Niehaves et al., 2012). Many companies use mobile device management (MDM) solutions which allow enforcing security policies even on employee-owned mobile devices. However, the complete implementation of corporate security policies limits the devices' functionality (e.g. by not allowing to install certain apps) which may not be tolerated by employees on their private devices. Consequently, regulations can usually not be enforced to the same extend on privately owned devices as on company owned devices. Therefore, privately owned devices provide a greater likelihood of potential violations of the corporate information security policies (Miller et al., 2012; Osterman Research, 2012). This results in two general threats to corporate information security: On the one hand, the integration of privately owned devices into corporate network facilitates malware intrusion (e.g. viruses, worms, trojans). On the other hand, it also increases the possibility of data loss and theft (Miller et al., 2012).

In terms of privacy concerns, Minch (2004) defines privacy as „the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." These concerns are related to a „possible loss of privacy as a result of information disclosure" (Krasnova, Kolesnikova and Günter, 2010). Similar to the aspect of information security, end user privacy concerns in the context of mobile device usage received plenty of attention from scholars (e.g. Figge, Schrott, Muntermann and Rannenberg, 2003; Ho, 2009). The existing academic literature mostly deals with the aspect of privacy of end users with regard to mobile service providers (e.g. mobile banking, mobile commerce, location-based services). Findings suggest that privacy concerns do affect an end user's acceptance of mobile services. Ho (2009) shows that end users may be afraid of being tracked and may worry that private data on their devices could be abused. In the context of BYOD, the privacy aspect refers to employees' concerns that private data (e.g. emails, photos, GPS data etc.) are exposed to the employer. Miller et al. (2012) suppose that the privacy aspect is potentially more important than the security aspect. The authors indicate that difficulties in differing between private and organizational data occur if employees use their privately owned devices in an organizational context. The installation of MDM software

---

[2] http://content.dell.com/us/en/corp/d/corp-comm/the-evolving-workforce

may be required to secure (e.g. virus protection), monitor, manage (e.g. data synchronization), and support BYOD mobile devices. This is why organizations could be able to track employees' locations during work and non-work hours, which applications they have installed and access personal data such as private emails and private photos (PR Newswire[3], 2012).

In addition to security and privacy concerns, the concept of BYOD is also associated with legal concerns (Osterman Research, 2012; Silvergate and Salner, 2011). In general information security research, the legal perspective is often linked to privacy (e.g. Earp, Anton and Jarvinen, 2002; Kayworth, Brocato and Witten, 2005). In this study, legal concerns refer to existing statutory regulations between employers and employees. For example, Silvergate and Salner (2011) indicate that the use of BYOD mobile devices causes violations of working hour regulations as employees "stay connected to their jobs on nights, weekends and even vacations". A consequence would be that employees demand compensation for their expanded working time (Silvergate and Salner, 2011). Furthermore, we assume that employees are concerned about being held liable if corporate information gets lost due to loss, theft or damage to their device.

Due to the importance of security, privacy, and legal concerns regarding BYOD, we propose the following hypothesis:

> H4: *Perceived uncertainty towards BYOD will be influenced significantly positive by (a) security concerns, (b) privacy concerns, and (c) legal concerns.*

DATA COLLECTION AND RESEARCH METHODOLOGY

For our empirical exploration, we designed an online survey and distributed it to employees of various German organizations via email and social networks (e.g. Xing, LinkedIn). The first two questions eliminated participants, who were neither employed nor privately owning a mobile device. These restrictions concerning the target group allowed to accurately measure the hypothesized constructs. To reduce bias, the questionnaire was provided in German language. Prior to the main test, seven pretests were conducted. The pretests were realized by means of intensive discussions with the participants in order to receive feedback concerning the validity and comprehensibility of the survey questions. Multiple item constructs were chosen using a five-point Likert scale, which ranged from „strongly disagree" to „strongly agree".

The survey was started by 298 people, of which 203 were employees (186 in possession of a mobile device). A total of 151 persons completed the survey. The majority of participants was at the age of 20-29, 83.5% stated their knowledge of computers and IT to be rather high/very high, and most of the participants (42.4%) work for a large-scale organization ($\geq$ 1000 employees) in the IT (27.8%), education (15.2%) and services (15.2%) industry. In terms of the information sensitivity of the organization, most of the participants (41.7%) indicated a very high level of information sensitivity. With regard to corporate permissions, 35.8% of the participants claimed that they are allowed to use BYOD mobile devices, while 64,2% declared they are not allowed to do so.

The statistical software program IBM SPSS Statistics version 20 (IBM[4], 2011) was used to conduct a rotated exploratory factor analysis (EFA) by means of a principal component analysis with varimax rotation. The results indicate convergent validity of the constructs (all factor loadings exceed 0.50 on their own construct) and discriminant validity (no cross loadings among the constructs that exceed 0.50) (van der Heijden, 2003). The internal consistency of the scales was further validated with the analysis of composite reliability (CR), which is similar to Cronbach's alphas, ranging from 0.93 to 0.98. To establish acceptable model reliability, the recommended values for CR are above 0.70 (Gefen, Straub and Boudreau, 2000). Another indicator for convergent and discriminant validity is the average variance extracted (AVE), ranging from 0.79 to 0.95. Fornell and Larcker (1981) recommend a lower limit of 0.50. In this study, the estimates exceed the recommended values for CR and AVE, indicating internal consistency of the scales as well as convergent and discriminant validity.

DISCUSSION AND IMPLICATIONS

To test the hypotheses, SmartPLS version 2.0.M3 (Ringle, Wende and Will[5], 2005) was used to conduct structural equation modeling (SEM). The t-values of the path coefficients were above 1.96 and 3.29, indicating a statistical significance with a probability of $p < .05$ and $p < .001$ (see Figure 1).

---

[3] http://www.prnewswire.com/news-releases/harris-survey-exposes-concerns-about-employee-privacy-for-byod-171520251.html

[4] ftp://public.dhe.ibm.com/software/analytics/spss/documentation/statistics/20.0/en/client/Manuals/IBM_SPSS_Statistics_Core_System_Users_Guide.pdf

[5] http://www.smartpls.de
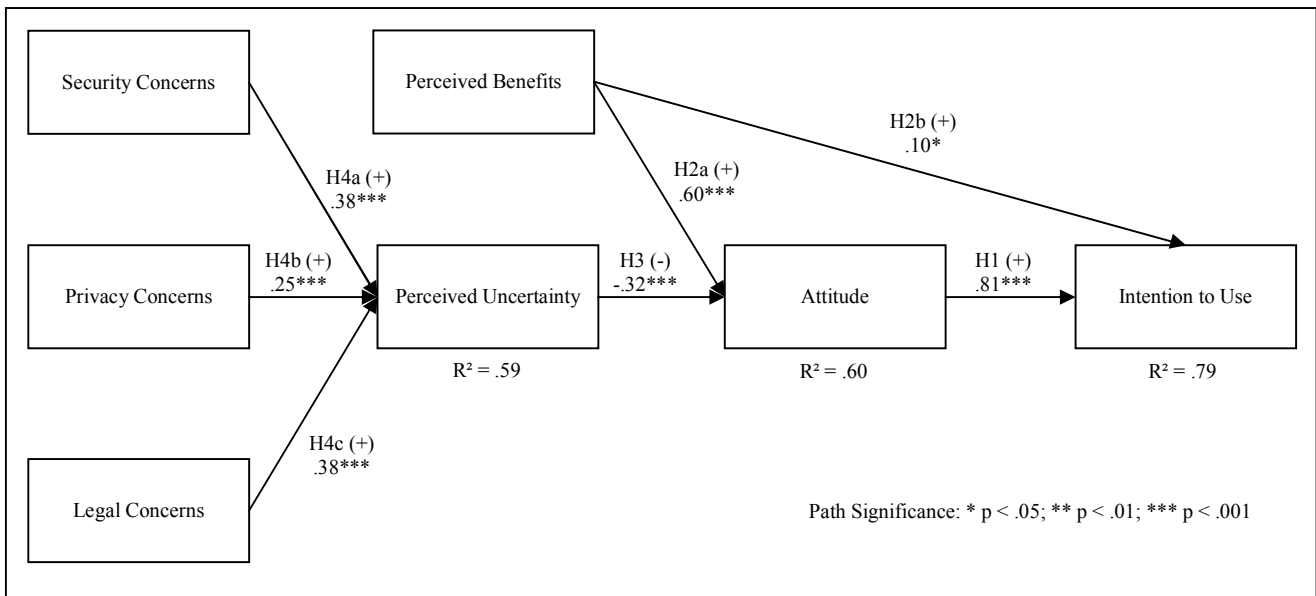
Figure 1: Results of the Structural Equation Modeling (SEM)

We found strong support for our theoretical model, as all hypotheses were supported with high significance based on data collected from N=151 employees who privately own a mobile device. As predicted by the TRA and the TAM, employees' intention to use BYOD mobile devices are significantly influenced by their attitude toward and perceived benefits of BYOD, explaining 79% of the variance of the construct. Furthermore, the results of this study show that both perceived benefits and perceived uncertainty significantly influence employees' attitude towards BYOD, explaining 60% of the construct's variance. Moreover, our study identified three classes of concerns that provide theoretical explanation for the antecedents of employees' uncertainty towards the concept of BYOD, explaining 59% of the variance of the construct: Security, privacy, and legal concerns. The theoretical contributions and practical implications of this study are discussed in the following.

Our study reveals a general indecision of employees towards BYOD. Based on a five-point Likert scale, the response mean values of each construct are within an interval of < .80 to the value 3. In contrast to the majority of market research studies, which discovered increased job satisfaction through the effects of BYOD (Niehaves et al., 2012), our theoretical study shows that employees are unsure as to whether using BYOD mobile devices would be beneficial. The same applies to employees' perceived uncertainty. Furthermore it is striking that employee attitude has a negative tending mean value (2.85), implying that employees have a slightly negative position towards BYOD. As hypothesized, both perceived benefits (.60, p < .001) and perceived uncertainty (-.32, p < .001) have a strong and significant effect on employees' attitude towards BYOD. However, the positive influence of perceived benefits clearly exceeds the negative impact of perceived uncertainty.

Consistent with the proposed research model, we found that employees' perceived uncertainty towards BYOD is largely due to security concerns, privacy concerns, and legal concerns. Regarding the beta values, it is to be noted that the influence of privacy concerns (.25) on perceived uncertainty is considerably lower than the influences of security concerns (.38) and legal concerns (.38). This trend is also evident with regard to the response mean values of the three concern constructs. Our study shows that employees are clearly more concerned about security (3.65) and the legal situation (3.43) than they are about their individual privacy (3.09). With regards to Miller et al. (2012), who supposed that the privacy aspect is potentially more important than the security aspect, our study reveals that employees have contradictory perceptions of this topic.

The results of this study provide important practical implications for organizations that are planning to implement a BYOD strategy. Organizations are dependent on employees' willingness to participate since BYOD is usually not mandatory. Consequently, employees' acceptance is crucial for implementing BYOD strategies. If organizations plan to implement a BYOD program, the slightly negative attitude of employees towards BYOD must change, because attitude is the main driver of intention. Our study shows that an increase in employee perception of the benefits of using BYOD mobile devices will have the greatest impact on their attitudes. Therefore we suggest that organizations should communicate and emphasize the advantages to their employees when planning to adopt the concept of BYOD. However, employees' perceived uncertainty plays an important role and cannot be neglected. Our findings show that perceived uncertainty is mainly impacted by

concerns towards security, privacy, and legal aspects. Organizations should focus on providing a secure infrastructure that allows employees to create, store, and manage corporate data from anywhere at any time using BYOD mobile devices. Additionally, a legal framework and privacy policies are needed to minimize employees' uncertainty.

LIMITATIONS AND FUTURE RESEARCH

Our study is subject to the following limitations: The first limitation relates to the sample used for this study, as it only consists of German employees. Consequently, we did not control for differences in culture. Leidner and Kayworth (2006) showed that national culture significantly impacts IS studies. Therefore the results of this study can only be generalized to other cultures with caution. We assume that cultural differences are of particular importance when analyzing the influences of security, privacy, and legal concerns, as relevant laws vary from country to country. Thus, future research is needed to analyze the cross-cultural influence of these two classes of concerns on employees' attitude towards BYOD. Another limitation related to the sample is its relatively small size, containing N=151 completed questionnaires. However, the partial least squares (PLS) analysis we used has minimal demands for sample size (Fornell and Larcker, 1981).

The focus of this study is on analyzing the impact of different types of concerns on employees' intention to use BYOD mobile devices. Consequently, the questionnaire emphasized the disadvantages of the BYOD concept, as it contained only five items regarding the benefits of the concept. Although the results nonetheless show that the influence of perceived benefits on employees' attitude is greater than the negative influence of perceived uncertainty, a possible bias due to questionnaire structure towards a negative attitude cannot be completely ruled out.

There are several further suggestions for future research: Since the proposed research model explains 59% of the variance of the perceived uncertainty construct, future research should focus on discovering additional constructs that influence employees' uncertainty towards BYOD. The same applies for the attitude construct, which can be explained to 60% by the proposed research model. Moreover, studies that focus more on benefits that drive employees' intention to use BYOD mobile devices are needed. We further recommend to investigate, to which degree the integration of BYOD mobile devices actually would increase employees' productivity and job satisfaction. Another aspect would be to examine, to which extent an integration actually would be cost-cutting for organizations, as costs may incur e.g. due to the implementation of MDM software. Moreover, it would be interesting to see how the potential for employer control of employees' personal devices via MDM might impact employees' perceived concerns.

CONCLUSION AND OUTLOOK

As the importance of mobile devices increased over the last several years, the trend of employees using their private mobile devices for working purposes emerged and is already beginning to impact organizations. As the concept of bring-your-own-device (BYOD) combines private ownership and organizational use, several advantages and concerns for both employees and organizations are discussed mainly in practical literature, whereas academic IS research literature presents little theoretical examination of the topic (Niehaves et al., 2012).

This study focused on analyzing the impact of perceived concerns on employees' intention to use BYOD mobile devices. Three classes of concerns that significantly impact employees' attitude towards the concept of BYOD were identified. The study revealed some unexpected results that contradict most of the practical literature. First, we showed that employees are undecided regarding their intention to use BYOD mobile devices. Second, we found that security aspects and the legal situation worry employees more than their individual privacy.

Our study highlights several implications for future research as well as for practitioners. Due to the ongoing discussion of the BYOD concept in practical literature and the lack of academic IS research literature in this area, we expect an increase in the practical and theoretical importance of the topic in the near future.

REFERENCES

1. Ajzen, I. (1991) The Theory of Planned Behavior, *Organizational Behavior and Human Decision Processes*, 50, 2, 179-211.

2. Beulen, E. and Streng, R.-J. (2002) The Impact of Online Mobile Office Applications on the Effectiveness and Efficiency of Mobile Workers Behavior: A Field Experiment in the IT Services Sector; *Proceedings of the 23rd International Conference on Information Systems,* December 15-18, Barcelona, Spain.

3. Davis, F.D. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quarterly*, 13, 3, 319-340.

4. Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. (1989) User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, *Management Science*, 35, 8, 982-1003.

5. Earp, J. B.; Anton, A. I. and Jarvinen, O. (2002) A Social, Technical and Legal Framework for Privacy management and Policies, *Proceedings of the Eighth Americas Conference on Information Systems*, August 9-11, Dallas, TX, USA.

6. Figge, S., Schrott, G., Muntermann, J. and Rannenberg, K. (2003) Earning Money - A Situation Based Approach for Mobile Business Models, *Proceedings of the 11th European Conference on Information Systems,* June 16-21, Naples, Italy.

7. Fishbein, M. and Ajzen, I. (1975) Belief, attitude, intention, and behavior: An introduction to theory and research, Addison-Wesley, Reading, MA, USA.

8. Fornell, C. and Larcker, D. (1981) Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research*, 18, 1, 39-50.

9. Friedman, J. and Hoffman, D.V. (2008) Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses, *Information Knowledge Systems Management*, 7-2008, 159–180.

10. Gefen, D., Straub, D.W. and Boudreau, M.-C. (2000) Structural Equation Modeling and Regression: Guidelines for Research Practice, *Communications of AIS*, 4, Article 7.

11. Giessmann, A.; Stanoevska-Slabeva, K. and de Visser, B. (2012) Mobile Enterprise Applications - Current State and Future Directions, *Proceedings of the 45th Hawaii International Conference on System Sciences*, January 4-7, Maui, HI, USA.

12. Harnesk, D. and Lindström, J. (2011) Shaping security behaviour through discipline and agility: Implications for information security management, *Information Management & Computer Security*, 19, 4, 262-276.

13. Herath, T. and Rao, H.R. (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations, *European Journal of Information Systems*, 18, 2, 106-125.

14. Ho, S. Y. (2009) Opportunities and Challenges of Mobile Personalization: An Exploratory Study, *Proceedings of the 17th European Conference on Information Systems*, June 8-10, Verona, Italy.

15. Johnson, N. and Joshi, K. D. (2012) The Pathway to Enterprise Mobile Readiness: Analysis of Perceptions, Pressures, Preparedness, and Progression, *Proceedings of the 18th Americas Conference on Information Systems*, August 8-9, Seattle, WA, Paper 18

16. Kayworth, T.; Brocato, L. and Witten, D. (2005) What is a Chief Privacy Officer? An AnalysisBased on Mintzberg's Taxonomy of Managerial Roles, *Communications of the Association for Information Systems*, 16-2005, 110-126.

17. Krasnova, H., Kolesnikova, E. and Günter, O. (2010) Leveraging Trust and Privacy Concerns in Online Social Networks: An Empirical Study, *Proceedings of the 18th European Conference on Information Systems*, June 6-9, South Africa, University of Pretoria.

18. Leidner, D. and Kayworth, T. (2006) „A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict," *MIS Quarterly*, (30:2), pp. 357-399.

19. Miller, K.W.; Voas, J. and Hulburt G.F. (2012) BYOD: Security and Privacy Considerations, *IT Professional*, 14, 5, 53-55.

20. Minch, R. P. (2004) Privacy Issues in Location-Aware Mobile Devices, *Proceedings of the 37th Hawaii International Conference on System Science,* January 5-8, Big Island, HI.

21. Moreno, C.; Tizon N. and Preda M. (2012) Mobile Cloud Convergence in GaaS: A Business Model Proposition, *Proceedings of the 45th Hawaii International Conference on System Sciences*, January 4-7, Maui, HI, USA.

22. Niehaves, B.; Köffer, S. and Ortbach, K. (2012) IT Consumerization – A Theory and Practice Review, *Proceedings of the 18th Americas Conference on Information Systems*, August 8-9, Seattle, WA, Paper 18.

23. Nysveen, H., Pedersen, P.E. and Thorbjørnsen, H. (2005) Intentions to Use Mobile Services: Antecedents and Cross-Service Comparisons, *Journal of the Academy of Marketing Science*, 33, 3, 330-346.

24. Oliver, R.L. and Bearden, W.O. (1985) Crossover Effects in the Theory of Reasoned Action: A Moderating Influence Attempt, *Journal of Consumer Research*, 12, 3, 324-340.

25. Osterman Research Inc. (2012) Putting IT Back in Control of BYOD, *Osterman Research White Paper*, June 2012, Black Diamond, WA, USA.

26. Pavlou, P.A., Liang, H. and Xue, Y. (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective, *MIS Quarterly*, 31, 1, 105-136.

27. Saari, L.M. and Judge, T.A. (2004) Employee Attitudes and Job Satisfaction, *Human Resource Management*, 43, 4, 395-407.

28. Scheepers, H. and Scheepers, R (2004) The Implementation of Mobile Technology in Organizations: Expanding Individual Use Contexts, *Proceedings of the 25th International Conference on Information Systems*, December 9-12, Charlottesville, VA, USA.

29. Silvergate, S.H. and Salner, D (2011) Smartphones and the Fair Labor Standards Act, *For the Defense – Legal Magazine*, June 2011, 41-44.

30. Spears, J.L. and Barki, H. (2010) User Participation in Information Systems Security Risk Management, *MIS Quarterly*, 34, 3, 503-522.

31. Taylor, S. and Todd, P.A. (1995) Understanding Information Technology Use: A Test of Competing Models, *Information Systems Research*, 6, 2, 144-176.

32. Tu, Z. and Yuan, Y (2012) Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft, *Proceedings of the 45th Hawaii International Conference on System Sciences*, January 4-7, Maui, HI, USA.

33. van der Heijden, H. (2003) Factors influencing the usage of websites: the case of a generic portal in The Netherlands, *Information & Management*, 40, 6, 541-549.

34. Venkatesh, V. and Davis, F.D. (1996) A Model of the Antecedents of Perceived Ease of Use: Development and Test, *Decision Sciences*, 27, 3, 451-481.

35. Zaplata, S., Kunze, C.P. and Lamersdorf, W. (2009) Context-based Cooperation in Mobile Business Environments – Managing the Distributed Execution of Mobile Processes, *Business & Information Systems Engineering*, 4-2009, 301-314.