

Legal and Privacy Concerns of BYOD Adoption

Kenan Degirmenci, Michael H. Breitner, Ferry Nolte & Jens Passlick

To cite this article: Kenan Degirmenci, Michael H. Breitner, Ferry Nolte & Jens Passlick (02 Oct 2023): Legal and Privacy Concerns of BYOD Adoption, Journal of Computer Information Systems, DOI: [10.1080/08874417.2023.2259346](https://doi.org/10.1080/08874417.2023.2259346)

To link to this article: <https://doi.org/10.1080/08874417.2023.2259346>



© 2023 The Author(s). Published with license by Taylor & Francis Group, LLC.



Published online: 02 Oct 2023.



Submit your article to this journal [↗](#)



Article views: 60



View related articles [↗](#)



View Crossmark data [↗](#)

Legal and Privacy Concerns of BYOD Adoption

Kenan Degirmenci ^a, Michael H. Breitner ^b, Ferry Nolte^c, and Jens Passlick^d

^aQueensland University of Technology, Brisbane, Queensland, Australia; ^bLeibniz University Hannover, Hannover, Germany; ^cContinental AG, Fort Mill, South Carolina, USA; ^dVHV Group, Hannover, Germany

ABSTRACT

We investigate legal concerns in privacy calculus, which are currently not given enough attention in privacy research. Legal aspects can lead to liability issues in various information systems scenarios such as bring your own device (BYOD) in the workplace. To analyze the impact of legal concerns in privacy calculus, we conducted a quantitative study by surveying 542 employees from three countries: United States, Germany, and South Korea. Building on our research model to test our hypothesized relationships, structural equation modeling was employed. Our findings provide recommendations for multinational organizations to mitigate legal concerns in privacy calculus. A comparison of the three countries reveals that employees from the United States and South Korea place greater emphasis on legal concerns compared to German employees. We develop an understanding of employees' concerns with liability issues, and how these affect their privacy calculus in a BYOD context.

KEYWORDS

Bring your own device; BYOD; IT consumerization; privacy calculus; legal concerns



Introduction

In the last several decades, there has been considerable discussion about privacy calculus, which explains that individuals disclose their personal information if benefits exceed risks, resulting in a risk—benefit trade-off analysis of information disclosure.^{1–4} While several antecedents of privacy concerns have been analyzed in the past, including privacy experiences, privacy awareness, personality differences, demographic differences, as well as culture and climate,⁵ legal concerns have played an underrated role so far. Although government regulation through law enforcement has been in the focus of some studies,⁶ employees' perceptions of liability issues have been largely overlooked. A possible breach of personal information emphasizes the importance of a potential threat of legal action.⁷ Therefore, BYOD is not only a challenge of information technology (IT) but also the concern of legal departments in organizations, because both employees and organizations are concerned with safeguarding themselves from liability issues.⁸

To investigate the role of legal concerns in privacy calculus, we focus on the case of bring your own device (BYOD), which has emerged with IT consumerization,⁹ achieving a rapid growth since 2012.¹⁰ While IT consumerization blurs the boundary between consumer and business technologies,¹¹ BYOD describes the use of employees' privately owned devices for work

purposes, e.g., to access corporate applications like e-mail and databases, or to create, store and manage corporate data.¹² Therefore, the phenomenon of BYOD is closely linked to the concept of IT consumerization. The use of BYOD increases employees' availability and thus the flexibility and mobility of the workforce when business needs occur.¹³ This flexibility allows employees to work from home or on the move with the result that business continuity increases significantly. This has substantially gained importance due to the global coronavirus disease 2019 (COVID-19) pandemic, which requires staff to increasingly work from home.

On the downside, BYOD is causing a “unique set of challenges for IT professionals”^{14(p1)} as it “redefines the relationship between employees (in terms of consumers of enterprise IT) and the IT organization.”^{15(p1)} Employees increasingly use their own devices and choose their own software, e.g., mobile apps, Skype or Dropbox, in addition to, or instead of, enterprise IT.¹⁶ The “anytime, anywhere”^{17(p504)} mind-set of mobile users favors the shift of employees' expectations away from traditional 9-to-5 office work toward flexible work hours and work location, which drives employees to use their mobile devices for work. This, in turn, alerts chief information officers (CIOs) to potential security risks for companies,¹⁸ such as the loss of devices that contain sensitive corporate data, data contamination through

CONTACT Kenan Degirmenci  kenan.degirmenci@qut.edu.au  School of Information Systems, Queensland University of Technology, 2 George Street, Brisbane, QLD 4000, Australia

© 2023 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

malware intrusion, data theft, or loss of control over corporate networks.¹⁹ Companies implement mobile device management (MDM) solutions in order to secure, monitor, manage, and support BYOD, which facilitates to establish IT-enabled work arrangements.²⁰ This concurrently allows companies to track employees' locations during work and non-work hours, which applications they have installed, and access personal data such as private e-mails and private photos. To that end, BYOD is prone to evoke employees' concerns about their privacy protection, which in turn hampers companies' BYOD strategies.

This raises the question of how organizations can effectively alleviate employees' privacy concerns, while protecting their personal data from any misuse. While the importance of legal concerns has been suggested in prior research in a BYOD privacy context,^{7,8} there is a lack of empirical investigation. In this paper, we analyze how employees' legal concerns affect their privacy calculus of BYOD benefits and risks, which influence their attitude and intention to use their own mobile devices for work. Our analysis of employees' BYOD legal concerns in a privacy calculus context enables recommendations for CIOs to develop BYOD strategies and policies. Since national culture can play an important role in individuals' behavior in organizational settings,²¹ we focus on the Anglo-American, European, and Asian culture and select three countries as typical examples for these cultures with high BYOD diffusion rates: United States, Germany, and South Korea.^{22,23} We enable CIOs to address differences in BYOD strategies for global operating companies. Our analysis contributes to research on IT consumerization focusing on one specific form, i.e., BYOD, and empirically testing employees' privacy calculus caused by companies' security measures, in our context the implementation of

MDM solutions. Our quantitative study focuses on the following research question:

RQ: How do employees' legal concerns affect their privacy calculus of benefits and risks of using their private mobile devices for work?

To address this research question, we develop our hypotheses and explain our research design. After our data collection, we conduct our data analysis and discuss the results of our structural equation modeling. We deduct findings and implications, explain recommendations and present limitations, a further research agenda and conclusions.

Research model and hypothesis development

We develop our research model and hypothesize relationships between legal concerns, BYOD benefits and risks (privacy calculus), as well as BYOD attitude and intention (Figure 1).

We build our empirical investigation on the privacy calculus theory,² which has been widely used in information systems (IS) research.^{1,24,25} In this regard, privacy is defined 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."^{26(p2)} To that end, privacy concerns are related to a "possible loss of privacy as a result of information disclosure."^{27(p4)} In the context of BYOD, the privacy aspect refers to employees' concerns that private data (e.g., e-mails, photos, GPS data, etc.) are exposed to the employer. Miller et al.²⁸ indicate that difficulties in conflict between private and organizational data occur if employees use their private devices in an organizational

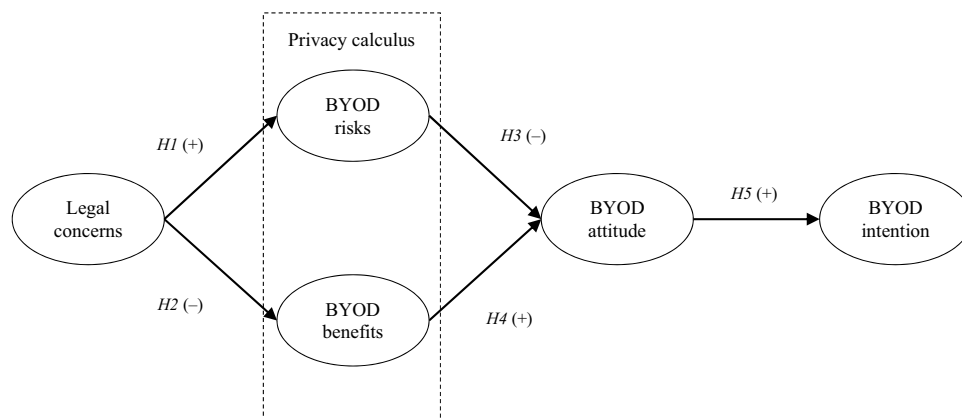


Figure 1. Research model.

context. Through the installation of MDM software, companies are able to track employees' personal information.

Since we are interested in the impact of legal concerns on the privacy calculus, we first focus on the risks associated with using private mobile devices for work. The role of legal concerns in privacy-related risks has been analyzed in other contexts, such as the Internet of things,²⁹ augmented reality,³⁰ cloud computing,³¹ electronic health records,³² biometrics,³³ or e-commerce.³⁴ In a BYOD context, we propose that employees' concerns with liability issues will hamper their BYOD adoption through increased perceptions of privacy risks. In information security research, the legal perspective is often linked to privacy.³⁵ From a privacy risk perspective, employees worry that their legal position in a company is threatened by exposing personal data to the employer such as their location, private photos, or text messages.

From a regulatory perspective, South Korea has published the Korean Personal Information Protection Act (PIPA), which is designed to safeguard individuals' rights and privacy by regulating the collection, processing, and use of their personal information.³⁶ Similarly, the European Union (EU) has implemented the General Data Protection Regulation (GDPR) requiring measures to protect EU citizens.³⁷ In the United States, the California Consumer Privacy Act (CCPA) has been passed in June 2018, mirroring the EU's GDPR.³⁸ Nevada, New York, and Washington, DC followed California's CCPA.³⁹ Like the EU GDPR, the CCPA focuses on the protection of citizens' data and targets all companies that handle any personally identifiable information of California residents.

With regard to benefits from personal information disclosure, there is scarce literature on the impact of legal concerns on workplace-related benefits such as job performance and productivity.⁴⁰ We propose that increased legal concerns through the introduction of BYOD in the workplace will evoke heightened stress, which will eventually lead to decreased productivity. From a privacy calculus perspective, we propose the following hypotheses:

H1: Employees' legal concerns are positively related to their perceptions of risks associated with the use of BYOD mobile devices.

H2: Employees' legal concerns are negatively related to their perceptions of benefits associated with the use of BYOD mobile devices.

Privacy risks are defined as "the degree to which an individual believes that a high potential for loss is associated with the release of personal information to

a firm,"^{5(p1001)} whereas privacy benefits refer to the anticipation that "individuals are assumed to behave in ways that they believe will result in the most favorable net level of outcomes."^{41(p363)} In our BYOD context, we expect that employees will perceive a potential for loss of their personal information to the employer through the use of BYOD mobile devices due to the employer's ability to track their personal information through MDM software, in turn affecting their technology adoption.⁴² With regard to benefits in the context of IT at the workplace, Davis⁴³ 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."^{43(p320)} 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."^{43(p320)} According to several studies, BYOD entails advantages for both employees and companies. For example, granting employees more privileges toward a more mobile workplace can increase the overall productivity within a company. Moreover, by allowing employees to choose their mobile work devices, their individual efficiency can be enhanced. A gain in employees' productivity and efficiency by higher job satisfaction can be the result of increased personal freedom since employees can use their preferred mobile devices in their favored locations and time. We hypothesize that employees' privacy calculus of risks and benefits associated with the use of BYOD mobile devices will affect their attitude:

H3: Employees' perceived risks are negatively related to the attitude toward using BYOD mobile devices.

H4: Employees' perceived benefits are positively related to the attitude toward using BYOD mobile devices.

Attitude is defined as "an individual's positive or negative feelings (evaluative affect) about performing the target behavior,"^{44(p984)} which is considered to be the most immediate antecedent of behavioral intention.⁴⁵ Ajzen⁴⁶ defines behavioral 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."^{46(p181)} In our context, employees' attitude will shape their intention to use BYOD mobile devices, which eventually will decide whether employees are willing to use their private mobile devices for work. While other studies investigate a direct influence of privacy concerns on the willingness to disclose personal

information,⁴⁷ we do not include that relationship for two reasons: (1) in contrast to these studies, where privacy concerns are situated on a more abstract level, we measure privacy concerns related specifically in a BYOD context, and (2) instead of information disclosure, our interest at this stage is on employees' usage of private mobile devices within the companies.

H5: Employees' attitude toward using BYOD mobile devices is positively related to the intention to use such devices.

Research design and results

Data collection

For our empirical analysis, we conducted a quantitative study with participants from different countries (United States, Germany, and South Korea) using an online survey (via social networking sites, e-mail, and personal recruitment through professional networking) and written submissions. Ethics approval was not required for this study because low-risk human research does not require ethics approval in the country where the study was conducted. We have chosen to examine differences among these cultures to additionally offer recommendations for global organizations, which comply with cross-cultural communication. We selected mature countries leading the IT sector: the United States as a representative country for the Anglo-American culture, Germany on behalf of the Central European culture, and South Korea representing the Asian culture. We found it suitable to compare these three nations due to a similar growing trend of BYOD usage and a similar share of mobile phone users.^{22,23} In fact, BYOD is not only an industry trend, but it has become integral to enterprise-wide operations and IT organizations.

The first two questions of the survey were designed to eliminate participants who were neither employed nor privately owned a mobile device. These restrictions concerning the target group allowed us to accurately measure the hypothesized constructs. To reduce bias, the questionnaire was provided in the English, German, and Korean languages (see Table A1 in the Appendix for the survey instrument). Prior to the main test, seven pretests were conducted. The pretests were realized by means of intensive discussions with the participants 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 four

items for legal concerns were self-developed based on McCrindle's⁴⁸ description of legal costs of conflict between employer and employee. The six-item scale of BYOD risks was used from Pavlou et al.,⁴⁹ who originally measured information privacy concerns of e-commerce customers, which we adapted in a BYOD context. BYOD benefits was measured with five items adapted from Davis,⁴³ who originally measured the perceived usefulness of IT to enhance job performance. BYOD attitude was measured with six items adapted from Nysveen et al.⁵⁰ and Taylor and Todd,⁵¹ and BYOD intention was measured with three items adapted from Venkatesh and Davis⁵² and Oliver and Bearden.⁵³

In total, 542 participants (i.e., employees from major cities in the United States, Germany, and South Korea) produced usable data, with 210 from the United States, 178 from Germany, and 154 from South Korea; requiring 11 minutes and 21 seconds on average to complete the survey. As shown in Table A2 in the Appendix, the responding participants (overall) were well represented in gender, age, size of the company, and industry, along with the participants' knowledge of computers and IT, and information sensitivity of the company. Nevertheless, there were some differences in demographic distribution. For example, more than half of the participants in the United States and Germany were in their 20s, but most Korean respondents were in their 30s and 40s. Still, most of the participants from all three countries reported that they were highly knowledgeable of computers and IT (see Table A2). Regarding industry, most German participants were working in IT, while most Korean participants were working in manufacturing. The manufacturing sector ranges from handcraft to high-technological manufacturing and smart applications play an increasing role in manufacturing. To control potential bias, we (1) *ex ante* conducted the survey based on random sampling, and (2) *ex post* performed a correlation analysis. Results showed that all correlations between the demographics and the latent variables were lower than 0.145, indicating very low correlations.⁵⁴ The correlation analysis indicated no confounding effects of the demographics on the latent variables, which is why such a bias can be excluded.

Data analysis

To test the research model, structural equation modeling (SEM) was conducted using partial least squares (PLS) path modeling with SmartPLS. SEM provides the ability to model relationships among multiple predictor and multiple criterion variables, which is why SEM is appropriate for

analyzing multivariate models.⁵⁵ In contrast to covariance-based SEM (CB-SEM), overall model fit indices such as the goodness of fit index (GFI) or the root mean square error of approximation (RMSEA) are not available in PLS-SEM, where the predictive validity is assessed by examining the R² and the structural paths.⁵⁵⁻⁵⁷ All indicators were modeled as being reflective of their respective constructs. Concerning the predictiveness of the model, factor loadings must be “at least 0.60 and ideally at 0.70 or above, indicating that each measure is accounting for 50% or more of the variance of the underlying LV [latent variable].”^{55(pxiii)} The measurement items in our model loaded between 0.712 and 0.951 on their respective constructs (see Table 1 for factor loadings), thus demonstrating adequate reliability. The internal consistency of the scales was validated with the analysis of Cronbach’s alpha ranging from 0.893 to 0.949, and composite reliability (CR) ranging from 0.926 to 0.961. To establish acceptable model reliability, the recommended values for construct reliability are above 0.70⁵⁶; the internal consistency criteria are therefore met. Average variance extracted (AVE) ranged from 0.721 to 0.878, Fornell and Larcker⁵⁸ recommend a lower limit of 0.50 for convergent validity.

To assess discriminant validity, we observed cross-loadings in the model and examined the Fornell-Larcker criterion. Accordingly, all items must load higher on their constructs than any cross-loadings on other constructs, and the square root of each construct’s AVE must be greater than its highest correlation with any other construct.⁵⁷ In all cases, the items loaded higher on their construct than they loaded on any other construct, and the differences were greater than 0.10, with most of them

Table 1. Loadings and cross loadings of measures.

	LEG	RISK	BEN	ATT	INT
LEG1	0.797	0.500	-0.058	-0.181	-0.174
LEG2	0.818	0.429	-0.082	-0.202	-0.182
LEG3	0.936	0.570	-0.017	-0.207	-0.222
LEG4	0.926	0.565	-0.023	-0.194	-0.208
RISK1	0.509	0.883	-0.016	-0.196	-0.234
RISK2	0.479	0.894	-0.004	-0.217	-0.249
RISK3	0.508	0.908	-0.050	-0.223	-0.190
RISK4	0.471	0.884	-0.060	-0.213	-0.223
RISK5	0.569	0.712	-0.125	-0.270	-0.206
RISK6	0.468	0.795	-0.015	-0.160	-0.148
BEN1	-0.068	-0.068	0.899	0.529	0.465
BEN2	-0.060	-0.061	0.934	0.554	0.443
BEN3	-0.000	-0.017	0.924	0.515	0.415
BEN4	-0.058	-0.040	0.911	0.522	0.440
BEN5	-0.029	-0.070	0.888	0.511	0.427
ATT1	-0.188	-0.235	0.518	0.923	0.647
ATT2	-0.233	-0.209	0.529	0.897	0.619
ATT3	-0.180	-0.204	0.529	0.925	0.655
ATT4	-0.123	-0.152	0.534	0.855	0.592
ATT5	-0.208	-0.270	0.495	0.889	0.638
ATT6	-0.254	-0.285	0.479	0.846	0.748
INT1	-0.214	-0.234	0.447	0.683	0.951
INT2	-0.218	-0.226	0.436	0.655	0.949
INT3	-0.206	-0.236	0.467	0.719	0.910

Table 2. Correlation matrix.

	LEG	RISK	BEN	ATT	INT
Legal concerns (LEG)	0.871				
BYOD risks (RISK)	0.597	0.849			
BYOD benefits (BEN)	-0.048	-0.057	0.912		
BYOT attitude (ATT)	-0.224	-0.256	0.578	0.889	
BYOT intention (INT)	-0.227	-0.248	0.481	0.734	0.937

greater than 0.19 (see Table 1 for loadings and cross loadings). Table 2 provides the correlation matrix with correlations among constructs and the square root of the AVE on the diagonal. The square root of the AVE for each construct is larger than the correlation of the construct with all other constructs in the model and the Fornell-Larcker criterion is met. Overall, the analysis of the data showed that reliability and validity quality criteria were met for our self-developed construct of legal concerns, as well as for the constructs of BYOD risks, benefits, attitude, and intention, where we adapted items from pre-validated measures.

Structural equation modeling

The hypotheses were tested by analyzing the structural equation modeling. By looking at the R² value, which explains the variance of the respective constructs, the explanatory power of the structural equation modeling can be evaluated. Figure 2 shows the results of the structural equation modeling for the combined data set including all three countries.

Legal concerns are found to be significantly influencing BYOD risks ($\beta = 0.597, t = 18.605$) and H1 is supported by our results. However, there is no significant impact of legal concerns on BYOD benefits ($\beta = -0.048, t = 1.032$), therefore, we could not find evidence to support H2. BYOD attitude is significantly influenced by BYOD risks ($\beta = -0.224, t = 5.929$) and BYOD benefits ($\beta = 0.565, t = 16.236$), supporting H3 and H4. Further, BYOD attitude is found to be significantly influencing BYOD intention ($\beta = 0.734, t = 29.850$) and H5 is supported.

To have a differentiated view of the differences between the three countries, we split the combined data set in a data set for the United States, Germany, and South Korea (see Table 3 showing the results for each country separately). Most interestingly, South Korea has the largest impact of legal concerns on BYOD risks. However, perceived risks of Korean employees are not significantly influencing their BYOD attitude. While BYOD benefits outweigh risks in all three countries, the discrepancy of the privacy calculus is larger in Germany and South Korea compared to the United States.

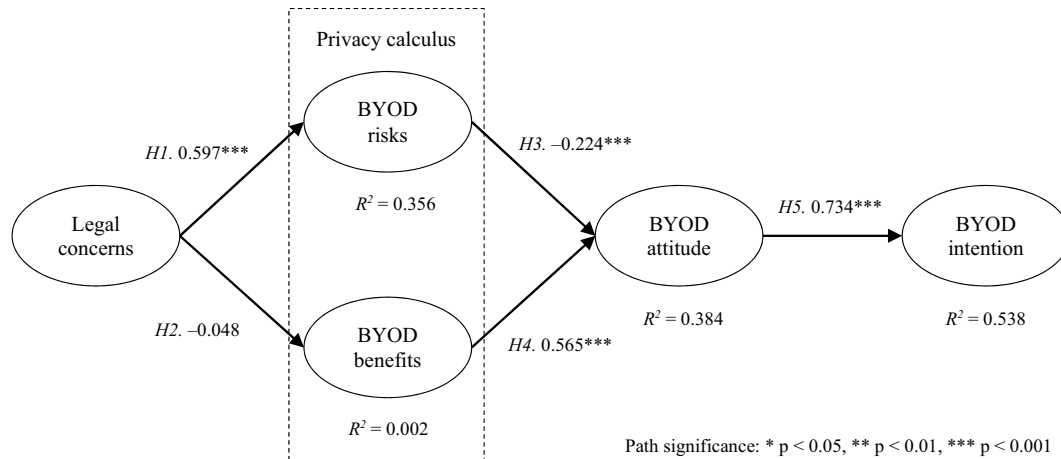


Figure 2. Results of structural equation modeling (combined data set).

Table 3. Results of structural equation modeling (split data set).

Path	USA		GER		KOR	
	β	t	β	t	β	t
LEG \rightarrow RISK	0.673***	14.828	0.438***	6.779	0.701***	17.437
LEG \rightarrow BEN	-0.072	1.092	-0.055	0.606	-0.120	1.511
RISK \rightarrow ATT	-0.376***	6.327	-0.182**	2.838	-0.039	0.548
BEN \rightarrow ATT	0.440***	7.422	0.653***	13.416	0.522***	6.761
ATT \rightarrow INT	0.681***	14.750	0.880***	47.249	0.582***	9.939

Path significance: * $p < .05$, ** $p < .01$, *** $p < .001$.

Discussion

Implications for research

Since our focus is on employees' privacy, we use the cultural dimensions to explain the discrepancy of the privacy calculus between the three cultures. As suggested by Hofstede et al.,⁵⁹ the United States is a highly individualist country (culture index: 91) compared to Germany (67), and South Korea (18) which represents the more collectivist culture. Individualist cultures represent "societies in which the ties between individuals are loose: everyone is expected to look after him- or herself and his or her immediate family. Collectivism as its opposite pertains to societies in which people from birth onward are integrated into strong, cohesive in-groups, which throughout people's lifetime continue to protect them in exchange for unquestioning loyalty."^{59(p92)} Most important here: in individualist countries, everyone has a right to privacy, whereas in collectivist cultures, private life is invaded by groups. We imply that the privacy calculus diverts substantially across different cultures: the predictive value of BYOD risks to explain the attitude toward BYOD is larger for highly individualist cultures such as the United States ($\beta = -0.376$, $p < .001$) compared to Germany ($\beta = -0.182$, $p < .01$) and to a highly

collectivist culture like South Korea ($\beta = -0.039$, $p > .05$). This is supported by the assumption that members of a collectivist society can rely on their collective network support, which is why they are less risk averse than those in an individualistic society.⁶⁰ Since the cultural dimension of uncertainty avoidance refers to a reduction of ambiguity instead of reducing risk,⁵⁹ we assume that employees from uncertainty-avoiding cultures are prepared to engage in risky behaviors such as using their private mobile device for work rather than waiting for the employer to initiate the process in order to reduce ambiguities.

At workplaces in large power distance cultures, managers generally rely on superiors and on formal rules, and subordinates expect to be told what to do, whereas in small power distance cultures, managers rely on their own experience and on subordinates, and subordinates expect to be consulted.⁵⁹ Broadly, power distance is defined as "the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally."^{59(p61)} In our study, employees' attitude toward BYOD from Germany as a small power distance culture (culture index: 35) has the highest impact on BYOD intention ($\beta = 0.880$, $p < .001$), followed by employees from the United States (power distance culture index:

40), whose attitude toward BYOD has the second-highest impact on BYOD intention ($\beta = 0.681$, $p < .001$), and employees from South Korea as a large power distance culture (60), whose BYOD attitude has the lowest impact on BYOD intention ($\beta = 0.582$, $p < .001$).

Implications for practice

Since cultural dimensions and cultural scores of the countries are viewed as a point of reference in the domestic population of a country,⁶¹ we additionally found implications from an organizational culture perspective, because organizational cultures are different in many respects from national cultures.⁵⁹ As Allen et al.⁶² show, organizational culture and organizational practices are interrelated and influence employee evasion when private information is disclosed. Furthermore, an organizational culture that is more flexibility-oriented fits organizational BYOD objectives and gives its employees fewer restriction and more empowerment, and thus less concerns regarding, e.g., organizational surveillance of private information.⁶³ Agreements between employee and employer are positively associated with reducing concerns, if they meet employee expectations and provide a secure feeling for the employees.⁶³ We recommend that further research more deeply examines which impact organizational culture has on privacy concerns associated with the implementation of BYOD and compare, e.g., the influence of different BYOD policies on privacy concerns.

Using mobile devices for work-related tasks has become a common practice among employees. For practical implications, it will be important for companies to understand differences of BYOD adoption between various types of groups regarding demographics such as gender, age, industry, and education level. Such understanding will help companies to develop their BYOD policies more appropriately, which will also help them to better address employees' legal and privacy concerns of BYOD adoption.

Finally, we found implications for BYOD privacy from a regulatory perspective. Several government regulations and regulatory compliances have been established to address the growing threats to privacy and security. From a practical perspective, i.e., considering government regulations and regulatory compliances, companies must react to employees' privacy concerns to comply with government regulations such as the PIPA, GDPR, and CCPA to avoid any legal complications through the implementation of BYOD. Further research can investigate whether regulatory initiatives, such as PIPA, GDPR, and CCPA, also create greater trust among employees in

the protection of their personal data and whether these initiatives reduce concerns about the use of BYOD.

Limitations and outlook for future research

One limitation relates to our sample used here, as it consists of American, German, and Korean employees. Consequently, we only discuss differences in these three cultures. Leidner and Kayworth⁶⁴ showed that national culture significantly impacts IS studies. Our results can only be generalized to other cultures with caution. In addition, we see that interdependencies between the multiple layers of culture exist, e.g., national layer, organizational layer, subunit layer or professional layer.⁶⁴ We interpret cultural differences by referring to Hofstede et al.'s⁵⁹ cultural index published in 2010, which is another limitation due to the time gap between their publication and our study. However, since changes in economic conditions and institutional characteristics are considered to influence cultural stability,⁶⁵ we do not assume that the cultural dimensions have changed substantially over time. In terms of generalizability, the limitation refers to a bias possibility of self-selection among the survey respondents.⁶⁶ The topic of the questionnaire revealed that the survey is about using private mobile devices for work purposes. Participants who responded may be those who are more likely to endorse BYOD and may also tend to be less concerned about their privacy. Another limitation regards to the challenge that BYOD policies can differ greatly among industries. Although we performed a correlation analysis, which showed no confounding effects of industry on the latent variables, we recommend that further research should focus on industry differences regarding legal and privacy concerns of BYOD adoption. Companies in finance and medical industries usually have strict policies about the security and privacy of corporate data and might be less willing to allow employees to use their personal devices to access company data.

Conclusions

As the importance of mobile devices has significantly increased over the last decade, the trend of employees using their private mobile devices for work has intensified and already begun to impact organizations. In IT consumerization, BYOD combines private ownership and organizational use. Several benefits and challenges for both employees and companies arise. Regarding our research question, we conducted a quantitative study and analyzed data from a survey with 542 employees from three cultures and representative countries, i.e., the

United States, Germany, and South Korea. Results of a structural equation modeling showed that BYOD risks are largely influenced by employees' legal concerns. American employees place greater emphasis on BYOD risks compared to employees from Germany and South Korea. Due to the growing "anytime, anywhere" mind-set of mobile users, we found that more and more employees expect flexible work hours rather than 9-to-5 office work. This, in turn, will consequently drive employees to use their private mobile devices for work, which leads companies to implement BYOD policies and MDM solutions to secure and monitor employees' private mobile devices. We expect that the role of employees' privacy concerns will further grow in importance, for which we provide recommendations for multinational organizations to face the growing pressure to integrate BYOD.


Acknowledgments

We dedicate this paper to our dear friend and colleague, J.P. Shim. He truly inspired this work, and his contributions, particularly regarding the multicultural aspect of the study, were pivotal for our research. J.P., you will be dearly missed. We thank Namyong Lee, Jongki Kim, and Joon Koh who supported collecting survey data from participants in South Korea. We are grateful for the constructive comments of the two anonymous reviewers. Finally, we thank Benedikt Lebek for his contributions to preliminary findings. Earlier versions of the paper were presented at the 19th Americas Conference on Information Systems and the 40th International Conference on Information Systems.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Kenan Degirmenci  <http://orcid.org/0000-0002-4046-4526>
Michael H. Breitner  <http://orcid.org/0000-0001-7315-3022>

References

- Culnan MJ, Armstrong PK. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organ Sci.* 1999;10(1):104–15. doi:10.1287/orsc.10.1.104.
- Laufer RS, Wolfe M. Privacy as a concept and a social issue: a multidimensional developmental theory. *J Soc Issues.* 1977;33(3):22–42. doi:10.1111/j.1540-4560.1977.tb01880.x.
- Lin J, Carter L, Liu D. Privacy concerns and digital government: exploring citizen willingness to adopt the COVIDSafe app. *Eur J Inform Syst.* 2021;30(4):389–402. doi:10.1080/0960085X.2021.1920857.
- Xu H, Teo H-H, Tan BCY, Agarwal R. The role of push-pull technology in privacy calculus: the case of location-based services. *J Manage Inform Syst.* 2009;26(3):135–73. doi:10.2753/MIS0742-1222260305.
- Smith HJ, Dinev T, Xu H. Information privacy research: an interdisciplinary review. *MIS Quart.* 2011;35(4):989–1015. doi:10.2307/41409970.
- Xu H, Teo H-H, Tan BCY, Agarwal R. Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Inform Syst Res.* 2012;23(4):1342–63. doi:10.1287/isre.1120.0416.
- Sipior JC, Bierstaker J, Chung Q, Lee J. A bring-your-own-device case for use in the classroom. *Commun AIS.* 2017;41:216–41. doi:10.17705/1CAIS.04110.
- Bello AG, Murray D, Armarego J. A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Inform Comput Secur.* 2017;25(4):475–92. doi:10.1108/ICS-03-2016-0025.
- Köffer S, Ortbach K, Junglas I, Niehaves B, Harris J. Innovation through BYOD? The influence of IT consumerization on individual IT innovation behavior. *Bus Inf Syst Eng.* 2015;57(6):363–75. doi:10.1007/s12599-015-0387-z.
- Sørensen C, Landau JS. Academic agility in digital innovation research: the case of mobile ICT publications within information systems 2000-2014. *J Strategic Inf Syst.* 2015;24(3):158–70. doi:10.1016/j.jsis.2015.07.001.
- Weeger A, Wang X, Gewalt H. IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *J Comput Inform Syst.* 2016;56(1):1–10. doi:10.1080/08874417.2015.11645795.
- Goel L, Zhang JZ, Williamson S. Work-to-home cybersecurity spillover: construct development and validation. *Inform Syst Manage.* 2022;1–11. doi:10.1080/10580530.2022.2128116.
- Doargajudhur MS, Dell P. The effect of bring your own device (BYOD) adoption on work performance and motivation. *J Comput Inform Syst.* 2020;60(6):518–29. doi:10.1080/08874417.2018.1543001.
- Johnson N, Joshi KD. The pathway to enterprise mobile readiness: analysis of perceptions, pressures, preparedness, and progression. *Proceedings of the 18th Americas Conference on Information Systems; 2012 Aug 9–12; Seattle, WA.* p. 1–8.
- Niehaves B, Köffer S, Ortbach K. IT consumerization – a theory and practice review. *Proceedings of the 18th Americas Conference on Information Systems; 2012 Aug 9–12; Seattle, WA.* p. 1–9.
- Junglas I, Goel L, Ives B, Harris J. Innovation at work: the relative advantage of using consumer IT in the workplace. *Inform Syst J.* 2019;29(2):317–39. doi:10.1111/isj.12198.
- Middleton C, Scheepers R, Tuunainen VK. When mobile is the norm: researching mobile information systems and mobility as post-adoption phenomena. *Eur J Inform Syst.* 2014;23(5):503–12. doi:10.1057/ejis.2014.21.
- Steelman ZR, Lacity M, Sabherwal R. Charting your organization's bring-your-own-device voyage. *Mis Q Exec.* 2016;15:85–104.

19. Palanisamy R, Norman AA, Mat Kiah ML. BYOD policy compliance: risks and strategies in organizations. *J Comput Inform Syst.* 2022;62(1):61–72. doi:10.1080/08874417.2019.1703225.
20. Lee J, Warkentin M, Crossler RE, Otondo RF. Implications of monitoring mechanisms on bring your own device adoption. *J Comput Inform Syst.* 2017;57(4):309–18. doi:10.1080/08874417.2016.1184032.
21. Ameen N, Tarhini A, Shah MH, Madichie NO. Employees' behavioural intention to smartphone security: a gender-based, cross-national study. *Comput Hum Behav.* 2020;104:1–14. doi:10.1016/j.chb.2019.106184.
22. Loucks J, Medcalf R, Buckalew L, Faria F. The financial impact of BYOD: a model of BYOD's benefits to global companies. CISCO; 2013 [accessed 2023 Sep 8]. https://www.cisco.com/c/dam/global/ru_ua/assets/pdf/byod-economics_econ_analysis.pdf.
23. Seo J. How to balance enterprise security with employee privacy. *Korea Times*; 2014 [accessed 2023 Sep 8]. https://www.koreatimes.co.kr/www/biz/2023/09/602_168246.html.
24. Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions. *Inform Syst Res.* 2006;17(1):61–80. doi:10.1287/isre.1060.0080.
25. Teubner T, Flath CM. Privacy in the sharing economy. *J Assoc Inf Syst.* 2019;20(3):213–42. doi:10.17705/1jais.00534.
26. Minch RP. Privacy issues in location-aware mobile devices. *Proceedings of the 37th Hawaii International Conference on System Sciences*; 2004 Jan 5–8; Waikoloa, HI. p. 1–10.
27. Xu H, Dinev T, Smith HJ, Hart P. Examining the formation of individual's privacy concerns: toward an integrative view. *Proceedings of the 29th International Conference on Information Systems*; 2008 December 14–17; Paris, France. p. 1–16.
28. Miller KW, Voas J, Hurlburt GF. BYOD: security and privacy considerations. *IT Prof.* 2012;14(5):53–55. doi:10.1109/MITP.2012.93.
29. Amiri-Zarandi M, Dara RA, Fraser E. A survey of machine learning-based solutions to protect privacy in the internet of things. *Comput Secur.* 2020;96:1–9. doi:10.1016/j.cose.2020.101921.
30. Rauschnabel PA, He J, Ro YK. Antecedents to the adoption of augmented reality smart glasses: a closer look at privacy risks. *J Bus Res.* 2018;92:374–84. doi:10.1016/j.jbusres.2018.08.008.
31. Cheng F-C, Lai W-H. The impact of cloud computing technology on legal infrastructure within internet—focusing on the protection of information privacy. *Procedia Engineer.* 2012;29:241–51. doi:10.1016/j.proeng.2011.12.701.
32. Thapa C, Camtepe S. Precision health data: requirements, challenges and existing techniques for data security and privacy. *Comput Biol Med.* 2021;129:1–23. doi:10.1016/j.combiomed.2020.104130.
33. Liu Y. Privacy regulations on biometrics in Australia. *Comput Law Secur Rev.* 2010;26(4):355–67. doi:10.1016/j.clsr.2010.05.002.
34. Zhu R, Srivastava A, Sutanto J. Privacy-deprived e-commerce: the efficacy of consumer privacy policies on China's e-commerce websites from a legal perspective. *Inform Technol Peopl.* 2020;33(6):1601–26. doi:10.1108/ITP-03-2019-0117.
35. Kayworth T, Brocato L, Whitten D. What is a chief privacy officer? An analysis based on mintzberg's taxonomy of managerial roles. *Commun AIS.* 2005;16:110–26. doi:10.17705/1CAIS.01606.
36. Ko H, Leitner J, Kim E, Jeong J. Structure and enforcement of data privacy law in South Korea. *Int Data Priv Law.* 2017;7(2):100–14. doi:10.1093/idpl/ix004.
37. Nadeau M. General data protection regulation (GDPR): what you need to know to stay compliant. *CSO*; 2020 [accessed 2023 Sep 8]. <https://www.csoonline.com/article/562107/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html>.
38. Korolov M. California consumer privacy act (CCPA): what you need to know to be compliant. *CSO*; 2020 [accessed 2023 Sep 8]. <https://www.csoonline.com/article/565923/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html>.
39. Serrato JK, Ross S. Nevada, New York and other states follow California's CCPA. *Norton Rose Fulbright*; 2019 [accessed 2023 Sep 8]. <https://www.dataprotectionreport.com/2019/06/nevada-new-york-and-other-states-follow-californias-ccpa>.
40. Yang H-C, Kim Y-E. The effects of corporate social responsibility on job performance: moderating effects of authentic leadership and meaningfulness of work. *J Asian Finance Econ Bus.* 2018;5(3):121–32. doi:10.13106/jafeb.2018.vol5.no3.121.
41. Stone EF, Stone DL. Privacy in organizations: theoretical issues, research findings, and protection mechanisms. *Res Pers Hum Res Man.* 1990;8:349–411.
42. Wang L, Sun Z, Dai X, Zhang Y, Hu H-H. Retaining users after privacy invasions: the roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Inform Technol Peopl.* 2019;32(6):1679–703. doi:10.1108/ITP-01-2018-0020.
43. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quart.* 1989;13(3):319–40. doi:10.2307/249008.
44. Davis FD, Bagozzi RP, Warshaw PR. User acceptance of computer technology: a comparison of two theoretical models. *Manage Sci.* 1989;35(8):982–1003. doi:10.1287/mnsc.35.8.982.
45. Fishbein M, Ajzen I. *Belief, attitude, intention, and behavior: an introduction to theory and research.* Reading (MA): Addison-Wesley; 1975.
46. Ajzen I. The theory of planned behavior. *Organ Behav Hum Dec.* 1991;50(2):179–211. doi:10.1016/0749-5978(91)90020-T.
47. Wu K-W, Huang SY, Yen DC, Popova I. The effect of online privacy policy on consumer privacy concern and trust. *Comput Hum Behav.* 2012;28(3):889–97. doi:10.1016/j.chb.2011.12.008.
48. McCrindle M. The costs of conflict. In: Falconer H, editor. *IRS managing conflict in the workplace.* London (UK):Routledge; 2004. pp. 37–59. doi:10.1016/B978-0-7545-2392-5.50007-5.
49. Pavlou PA, Liang H, Xue Y. Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. *MIS QUART.* 2007;31(1):105–36. doi:10.2307/25148783.

50. Nysveen H, Pedersen PE, Thorbjørnsen H. Intentions to use mobile services: antecedents and cross-service comparisons. *J Acad Market Sci.* 2005;33(3):330–46. doi:10.1177/0092070305276149.
51. Taylor S, Todd PA. Understanding information technology usage: a test of competing models. *Inform Syst Res.* 1995;6(2):144–76. doi:10.1287/isre.6.2.144.
52. Venkatesh V, Davis FD. A model of the antecedents of perceived ease of use: development and test. *Decision Sci.* 1996;27(3):451–81. doi:10.1111/j.1540-5915.1996.tb01822.x.
53. Oliver RL, Bearden WO. Crossover effects in the theory of reasoned action: a moderating influence attempt. *J Consum Res.* 1985;12(3):324–40. doi:10.1086/208519.
54. Hinkle DE, Wiersma W, Jurs SG. *Applied statistics for the behavioral sciences.* 2nd. Boston (MA): Houghton Mifflin Company; 1988.
55. Chin WW. Issues and opinion on structural equation modeling. *MIS QUART.* 1998;22:vii–xvi.
56. Gefen D, Straub DW, Boudreau M-C. Structural equation modeling and regression: guidelines for research practice. *Commun AIS.* 2000;4(7):1–77. doi:10.17705/1CAIS.00407.
57. Hair JF, Jr., Hult GTM, Ringle CM, Sarstedt M. *A primer on partial least squares structural equation modeling (PLS-SEM).* 2nd. Thousand Oaks (CA): Sage Publications; 2017.
58. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. *J Marketing Res.* 1981;18(1):39–50. doi:10.1177/002224378101800104.
59. Hofstede G, Hofstede GJ, Minkov M. *Cultures and organizations: software of the mind – intercultural cooperation and its importance for survival.* 3rd. New York (NY): McGraw-Hill; 2010.
60. Hsee CK, Weber EU. Cross-national differences in risk preference and lay predictions. *J Behav Decis Making.* 1999;12(2):165–79. doi:10.1002/(SICI)1099-0771(199906)12:2<165:AID-BDM316>3.0.CO;2-N.
61. Jones M, Alony I. The cultural impact of information systems – through the eyes of Hofstede – a critical journey. *Issues Inform Sci Inf Technol.* 2007;4(1):407–19. doi:10.28945/960.
62. Allen MW, Coopman SJ, Hart JL, Walker KL. Workplace surveillance and managing privacy boundaries. *Manage Commun Q.* 2007;21(2):172–200. doi:10.1177/0893318907306033.
63. Chang SE, Liu AY, Lin S. Exploring privacy and trust for employee monitoring. *Ind Manage Data Syst.* 2015;115(1):88–106. doi:10.1108/IMDS-07-2014-0197.
64. Leidner DE, Kayworth T. A review of culture in information systems research: toward a theory of information technology culture conflict. *MIS Quart.* 2006;30(2):357–99. doi:10.2307/25148735.
65. Tang L, Koveos PE. A framework to update Hofstede’s cultural value indices: economic dynamics and institutional stability. *J Int Bus Stud.* 2008;39(6):1045–63. doi:10.1057/palgrave.jibs.8400399.
66. Kankanhalli A, Tan BCY, Wei K-K. Contributing knowledge to electronic knowledge repositories: an empirical investigation. *MIS QUART.* 2005;29(1):113–43. doi:10.2307/25148670.

Appendix

Table A1. Survey instrument.

Items	English	German	Korean
Legal concerns (LEG), Source: Self-developed			
	If I would use my personal mobile device to create, store and manage sensitive corporate data...	Wenn ich mein persönliches mobiles Endgerät für das Erstellen, Speichern und Verwalten von sensiblen Unternehmensdaten nutzen würde...	만일 나의 개인 모바일기기로 회사의 중요한/민감한 자료를 처리/다룬다면 (저장, 관리등)...
LEG1	I would be concerned that legal conflicts could emerge, for example, work time regulation, account of charges, commitment to maintenance, etc.	wäre ich besorgt, dass rechtliche Konflikte entstehen könnten, z. B. Arbeitszeitregelung, Kostenabrechnung, Wartungsverpflichtung usw.	작업시간 규제등 법적인 문제가 발생할수도 있다고 걱정된다.
LEG2	it would bother me that my employer could assert a legal claim against me.	würde es mich stören, dass mein Arbeitgeber Rechtsansprüche gegen mich geltend machen könnte.	나의 고용주가 나에게 대해 법적대응을 할 수 있다고 나를 괴롭힌다.
LEG3	I would be concerned about legal aspects.	wäre ich über rechtliche Aspekte besorgt.	법적인 측면을 걱정한다.
LEG4	I would have doubts as to how well my legal position is protected.	hätte ich meine Zweifel, ob meine rechtliche Situation geschützt ist.	나의 법적보호에 대해 걱정한다.
BYOD risks (RISK), Source: Pavlou et al.⁴⁹			
	If I would use my private mobile device to create, store and manage sensitive corporate data...	Wenn ich mein privates mobiles Endgerät für das Erstellen, Speichern und Verwalten von sensiblen Unternehmensdaten nutzen würde...	만일 나의 개인 모바일기기로 회사의 중요한/민감한 자료를 처리/다룬다면 (저장, 관리등)...
RISK1	I would be concerned that my employer is collecting too much information about me, for example, profiles of social networks, private e-mails, private photos, etc.	wäre ich besorgt, dass mein Arbeitgeber zu viele Informationen über mich erfasst, z. B. Profile auf sozialen Netzwerken, private E-Mails, private Fotos usw.	나의 고용주가 나의 개인 이메일, 사진, 소셜네트워크등에 관한 정보수집을 하리라 걱정된다.
RISK2	I would be concerned about my privacy.	wäre ich über meine Privatsphäre besorgt.	나의 비밀(프라이버시)에 걱정된다.
RISK3	my personal information could be misused.	könnten meine persönlichen Informationen missbraucht werden.	나의 개인정보가 오용되리라 생각한다.
RISK4	I would have doubts as to how well my privacy is protected.	hätte ich meine Zweifel, ob meine Privatsphäre geschützt ist.	나의 비밀(프라이버시)를 어떻게 보호해야 할지 생각해본다.
RISK5	it would bother me that my employer could scan my personal data.	würde es mich stören, wenn mein Arbeitgeber persönliche Informationen abfragen könnte.	나의 고용주가 내 개인정보를 스캔할 수도 있음에 괴롭히게 한다.
RISK6	my personal information could be accessed by unknown parties.	könnten sich unbekannte Dritte Zugang zu meinen persönlichen Informationen verschaffen.	나의 개인정보가 모르는 사람에게 접근될수도 있다.
BYOD benefits (BEN), Source: Davis⁴³			
	Using my private mobile device for work purposes would...	Mein privates mobiles Endgerät für berufliche Zwecke zu nutzen würde...	직장일을 하는데 개인 모바일 기기사용이...
BEN1	enable me to accomplish my tasks more quickly.	es mir ermöglichen, meine Aufgaben schneller zu erledigen.	나의 업무를 빨리 마치게 한다.
BEN2	improve my job performance.	meine Arbeitsleistung verbessern.	나의 직무성과를 개선한다.
BEN3	increase my productivity.	meine Produktivität erhöhen.	나의 생산성을 제고한다.
BEN4	enhance my effectiveness on the job.	meine Leistungsfähigkeit steigern.	직무효과를 증진한다.
BEN5	make it easier for me to do my job.	es mir erleichtern, meine Aufgaben zu erledigen.	직무를 하는데, 쉬워진다.
BYOD attitude (ATT), Sources: Nysveen et al.⁵⁰; Taylor and Todd⁵¹			
	Using my private mobile device for work purposes...	Mein privates mobiles Endgerät für berufliche Zwecke zu nutzen...	직무를 하는데, 나의 개인 모바일 기기를 사용함이...
ATT1	is a good idea.	ist eine gute Idee.	좋은 생각이다.
ATT2	is a wise idea.	ist eine kluge Idee.	현명한 생각이다.
ATT3	would be positive.	wäre positiv.	긍정적이다.
ATT4	would be beneficial.	wäre vorteilhaft.	혜택을 볼 수 있다.
ATT5	would be favorable.	wäre angenehm.	우호적이다.
ATT6	I like the idea of using my private mobile device for work purposes.	Mir gefällt die Vorstellung, mein privates mobiles Endgerät für berufliche Zwecke zu nutzen.	직무를 하는데, 나의 개인 모바일 기기 사용하는 아이디어를 나는 좋아한다.
BYOD intention (INT), Sources: Venkatesh and Davis⁵²; Oliver and Bearden⁵³			
INT1	Assuming I have my employer's permission, I would use my private mobile device for work purposes.	Angenommen ich hätte die Erlaubnis von meinem Arbeitgeber, würde ich mein privates mobiles Endgerät für berufliche Zwecke nutzen.	나의 고용주의 허락을 받는다고 가정할 경우, 나는 직무를 위해, 나의 개인 모바일 기기를 사용하고저 한다.
INT2	Given that I have my employer's permission to use my private mobile device for work purposes, I predict that I would use it.	Sollte mein Arbeitgeber mir die Erlaubnis zur Nutzung meines privates mobilen Endgerätes für berufliche Zwecke erteilen, würde ich dies wahrnehmen.	나의 고용주의 허락을 받았다고 할 경우, 나는 직무를 위해, 나의 개인 모바일 기기를 사용할것 같다 (예측한다)
INT3	How probable is it that you would use your private mobile device for work purposes, assuming that you have your employer's permission?	Wie wahrscheinlich ist es, dass Sie Ihr privates mobiles Endgerät für berufliche Zwecke nutzen würden, wenn Sie die Erlaubnis Ihres Arbeitgebers hätten?	나의 고용주의 허락을 받는다고 가정할 경우, 나는 직무를 위해, 나의 개인 모바일 기기를 얼마나 사용하리라 생각하는가?

Table A2. Profiles of responding participants.

	USA (N = 210)		GER (N = 178)		KOR (N = 154)		ALL (N = 542)	
Gender								
Male	54	25.7%	101	56.7%	122	79.2%	277	51.1%
Female	137	65.2%	57	32.0%	31	20.1%	225	41.5%
Not specified	19	9.0%	20	11.2%	1	0.6%	40	7.4%
Age								
≤19	0	0.0%	0	0.0%	0	0.0%	0	0.0%
20–29	108	51.4%	101	56.7%	13	8.4%	222	41.0%
30–39	38	18.1%	34	19.1%	60	39.0%	132	24.4%
40–49	29	13.8%	17	9.6%	54	35.1%	100	18.5%
50–59	12	5.7%	5	2.8%	25	16.2%	42	7.7%
≥60	4	1.9%	1	0.6%	2	1.3%	7	1.3%
Not specified	19	9.0%	20	11.2%	0	0.0%	39	7.2%
Participants' knowledge of computers and IT								
1 (Very low)	5	2.4%	8	4.5%	1	0.6%	14	2.6%
2	16	7.6%	9	5.1%	1	0.6%	26	4.8%
3	16	7.6%	8	4.5%	14	9.1%	38	7.0%
4	113	53.8%	67	37.6%	89	57.8%	269	49.6%
5 (Very high)	41	19.5%	66	37.1%	47	30.5%	154	28.4%
Not specified	19	9.0%	20	11.2%	2	1.3%	41	7.6%
Size of the organization (# of employees)								
≤9	24	11.4%	6	3.4%	5	3.2%	35	6.5%
10–49	46	21.9%	30	16.9%	23	14.9%	99	18.3%
50–249	29	13.8%	22	12.4%	42	27.3%	93	17.2%
250–499	20	9.5%	19	10.7%	16	10.4%	55	10.1%
500–999	10	4.8%	11	6.2%	15	9.7%	36	6.6%
≥1000	62	29.5%	70	39.3%	53	34.4%	185	34.1%
Not specified	19	9.0%	20	11.2%	0	0.0%	39	7.2%
Industry								
Education	13	6.2%	23	12.9%	14	9.1%	50	9.2%
Financial Services	9	4.3%	9	5.1%	9	5.8%	27	5.0%
Government	8	3.8%	3	1.7%	19	12.3%	30	5.5%
Food/Beverage/CPG	12	5.7%	2	1.1%	1	0.6%	15	2.8%
Health Care	20	9.5%	11	6.2%	1	0.6%	32	5.9%
Manufacturing	5	2.4%	14	7.9%	43	27.9%	62	11.4%
Nonprofit	13	6.2%	3	1.7%	10	6.5%	26	4.8%
Medical, Bio-Technology, Pharmacology	5	2.4%	5	2.8%	0	0.0%	10	1.8%
Real Estate	4	1.9%	0	0.0%	1	0.6%	5	0.9%
Services	13	6.2%	23	12.9%	18	11.7%	54	10.0%
Information Technology	18	8.6%	46	25.8%	16	10.4%	80	14.8%
Telecommunications	6	2.9%	2	1.1%	0	0.0%	8	1.5%
Travel	1	0.5%	3	1.7%	0	0.0%	4	0.7%
Wholesale/Retail	10	4.8%	3	1.7%	3	1.9%	16	3.0%
Other	54	25.7%	11	6.2%	18	11.7%	83	15.3%
Not specified	19	9.0%	20	11.2%	1	0.6%	40	7.4%
Information sensitivity of the organization								
1 (Very low information sensitivity)	6	2.9%	0	0.0%	0	0.0%	6	1.1%
2	34	16.2%	24	13.5%	25	16.2%	83	15.3%
3	21	10.0%	20	11.2%	22	14.3%	63	11.6%
4	82	39.0%	48	27.0%	85	55.2%	215	39.7%
5 (Very high information sensitivity)	48	22.9%	66	37.1%	22	14.3%	136	25.1%
Not specified	19	9.0%	20	11.2%	0	0.0%	39	7.2%