Future of Flexible Work in the Digital Age: Bring Your Own Device Challenges of Privacy Protection

Completed Research Paper

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

J.P. Shim
Department of Computer Information Systems, Georgia State University
Atlanta, GA, United States
jpshim@gsu.edu

Michael H. Breitner
Information Systems Institute
Leibniz University Hannover
Hannover, Germany
breitner@iwi.uni-hannover.de

Ferry Nolte
Information Systems Institute
Leibniz University Hannover
Hannover, Germany
nolte@iwi.uni-hannover.de

Jens Passlick
Information Systems Institute
Leibniz University Hannover
Hannover, Germany
passlick@iwi.uni-hannover.de

Abstract

The future of work is getting increasingly flexible due to the rising expectations of employees away from traditional 9-to-5 office work towards flexible work hours, which drives employees to use their mobile devices for work. This ever-growing phenomenon of Bring Your Own Device (BYOD) creates security risks for companies, which leads to an implementation of mobile device management (MDM) solutions to secure and monitor employees' mobile devices. We present insights from two multinational case companies, where works councils have expressed their concerns for privacy intrusion into employees' lives through BYOD. To examine whether employees share works councils' concerns, we conducted a survey with 542 employees from three countries: United States, Germany, and South Korea. Results of a structural equation modeling show that American employees place greater emphasis on BYOD risks associated with privacy concerns compared to employees from Germany and South Korea.

Keywords: Bring Your Own Device (BYOD), IT consumerization, IT-enabled work arrangements, policies and regulations for digital work, mobile devices, privacy

Introduction

Bring Your Own Device (BYOD) has emerged with the consumerization of information technology (IT) (Bygstad 2017; French et al. 2014; Karanasios and Allen 2014; Köffer et al. 2015; Middleton et al. 2014; Schmitz et al. 2016; Spagnoletti et al. 2015; Steinbart et al. 2016; Warkentin et al. 2016), achieving a rapid growth since 2012 (Sørensen and Landau 2015). A global report shows that the BYOD and enterprise mobility market is estimated to grow from $35.10 billion in 2016 to $73.30 billion by 2021 (MarketsandMarkets 2016). BYOD describes the use of employees' privately owned devices for work purposes (Lee Jr. et al. 2013; Loose et al. 2013), e.g., to access corporate applications like email and databases, or to create, store and manage corporate data (Osterman Research 2012). BYOD is often linked to several advantages and challenges for both employees and companies. From an employee's point of view, advantages are an increased degree of flexibility and motivation, as well as easier technology adoption (Niehaves et al. 2012). These benefits can lead to a higher job satisfaction (Osterman Research 2012). Since positive job satisfaction increases employees' productivity (Saari and Judge 2004), companies can benefit from BYOD (Dell 2011; Osterman Research 2012). The use of BYOD increases employees' availability and thus the flexibility and mobility of the workforce when business needs occur. This flexibility allows employees to work from home or on the move with the result that business continuity increases significantly. But, there are also BYOD challenges, which create a "unique set of challenges for IT professionals" (Johnson and Joshi 2012, p. 1) as it "redefines the relationship between employees (in terms of consumers of enterprise IT) and the IT organization" (Niehaves et al. 2012, p. 1). 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 (Junglas et al. 2019). The "anytime, anywhere" mindset of mobile users (Middleton et al. 2014; Picoto et al. 2014; Saha and Mukherjee 2003) favors the shift of employees' expectations away from traditional 9-to-5 office work towards flexible work hours and work location (Meeker 2015), which drives employees to use their mobile devices for work. This, in turn, alerts chief information officers (CIOs) to potential security risks for companies (Steelman et al. 2016), such as the loss of devices that contain sensitive corporate data, data contamination through malware intrusion, data theft, or loss of control over corporate networks (Tu and Yuan 2015). Companies implement mobile device management (MDM) solutions in order to secure, monitor, manage, and support BYOD, which facilitates to establish IT-enabled work arrangements (Eze Castle Integration 2018). 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 emails and private photos (PR Newswire 2012). To that end, BYOD is prone to evoke employees' concerns about their privacy protection, which in turn hampers companies' BYOD strategies.

We analyze how employees' privacy concerns substantially affect their privacy calculus of BYOD benefits and risks, which influence their attitude and decide over their intention to use their own mobile devices for work. Our analysis of employees' BYOD privacy concerns enables recommendations for CIOs to develop BYOD strategies and policies. 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 (Cisco 2013; IDG Connect 2014). Thus, 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 study focuses on two research questions: (1) How do companies deal with employees' privacy concerns regarding the introduction of BYOD? (2) What is the impact of employees' privacy calculus of risks and benefits associated with the use of BYOD mobile devices on their attitude and in turn intention to use their private mobile devices for work?

We acknowledge that prior studies exist which focus on the privacy calculus of IT usage in different contexts, such as health IT (Zhang et al. 2018), mobile app downloads (Wottrich et al. 2018), or Internet of things services (Kim et al. 2019). Our study provides a novel approach for two reasons. First, while these prior studies have a consumer perspective, we first investigate how works councils deal with employees' privacy concerns from an organizational perspective from two case companies, and then examine employees' privacy concerns to provide empirical justification for the actions taken by the works councils to protect employees' privacy. Second, while investigating works councils from multinational

corporations, we provide insights from our empirical analysis from three different countries and provide implications from a cultural differences perspective.

We first describe the process of BYOD implementation in two real-world companies and how works councils address privacy concerns as part of the development process to introduce policies and regulations for digital work. We build on the two cases to investigate whether employees share the works councils' concerns by conducting a survey with employees from three countries. We discuss the underlying theories for our survey research, develop hypotheses, and explain our research design, in which we describe our data collection, data analysis, and results of a structural equation modeling. We discuss findings and outline implications, recommendations, and limitations, followed by conclusions and an outlook.

Real-World BYOD Security Management and Privacy Intrusion

In recent literature, BYOD has been related to the challenge of securing corporate data and protecting private information due to employees' usage of private mobile devices in companies (Schmitz et al. 2016). In a guest editorial of the *European Journal of Information Systems*, Middleton et al. (2014) have emphasized that the "BYOD contextual overlap essentially swaps the private and work context around" (p. 509), and they stressed on the importance of the risks from an organizational perspective of opening up the computing infrastructure to private use. In this regard, security policies are considered as a crucial factor to create organizational standards for BYOD implementation and overcome security breaches (Ortbach et al. 2015; Putri and Hovav 2014). Since mobile devices such as smartphones and tablets are most commonly used for BYOD practices (Cisco 2013), it is important to consider the specific characteristics of the BYOD environment. For example, Steinbart et al. (2016) suggest that "secure authentication policies that are effective in the desktop computing paradigm will not work in the mobile paradigm" (p. 234) and report that many employees do not configure their mobile devices to require any form of authentication.

These concerns from an organizational perspective motivated us to have a deeper look into two real-world case companies, where BYOD policies have been discussed in the works council from an organizational security perspective, but also from an employee privacy perspective. Both case companies have dealt with the topic of private device security management and the privacy intrusion questions that arose from an employee standpoint.

The first case in which BYOD introduction was slowed down by privacy concerns was a German-based multinational corporation in the automotive industry with around 250,000 employees. The BYOD initiative originated in the company's workplace of the future program which was started in 2010. The program deals with the digital transformation of the office workspace for employees and targets to increase work flexibility for employees and to strengthen collaboration and knowledge sharing among employees. As part of the program, the corporations introduced several new information and communication technologies like enterprise social media which initiated some of the ideas within the IT organization to incorporate a BYOD possibility. With BYOD, the corporation aims to provide the benefits of new technologies to employees who are not eligible to use a company phone, or for managers who want to connect a private smartphone or tablet to the company account. However, in the first case company, such new practices need to be agreed upon with the works council before the implementation can be undertaken for the majority of employees (e.g., managing positions are not under works council government). In the first case company, members of the works council raised concerns over employees' personal data protection, how private devices will be altered to comply with corporate security policies, who has access to the data, employee protection in regard to work-life balance interference (e.g., always on work style) and how to deal with phone incidents that occur while using the private devices for work-related topics. In 2014, a corporation-wide agreement was reached that regulates consequences to private devices that are enrolled in the BYOD program. It was decided that the devices will be treated in the same way as corporate devices, meaning device properties will be altered by administrators that restrict certain uses (e.g., app installations restrictions) and allowing administrators access to the phone data. This intrusion of privacy of private devices is regulated in key paragraphs of the agreement that aims at the protection of personal data, restriction of performance evaluation based on collected mobile data and corporate access to the phone. It is clearly stated that access is only provided for IT support, the data can only be viewed by administrators, and the retrieval of collected data needs to be run by the works council

for approval. The employee cannot be evaluated on any collected data and the management needs to provide all sources of information that a negative personnel evaluation is based on. The employee that enrolls to BYOD is not legally actionable other than the employee does act on willful intent or in case of gross negligence. In addition, the works council has the right to request access to the collected data without a formal request at any given time and the storage of the data is only allowed on company-owned servers that are used exclusively for the MDM operations. Considering these organizational regulations that protect employees' rights, the first case company approved the use of BYOD, which is still in the worldwide roll-out. Every employee that enrolls in the program needs to sign a form that educates about the restrictions and the corporate access rights that come with it. The first case highlights that the company has a focus on the protection of personal data and privacy of employees that want to enroll in the BYOD program.

The second case company is an international engineering and manufacturing company headquartered in Germany with branches in 60 countries worldwide. The main business is automation products and systems. With approximately 3,700 employees worldwide, this company is smaller, but there are similar concerns about data protection, which have been increased through the introduction of a new MDM system to the company in 2013. The old MDM system had several disadvantages, for example, the mail client could not be sufficiently secured and the company apps were not sufficiently isolated from other apps. The new system, which is currently in use, allows finer differentiation of these settings. Company data is stored in company apps that run separately from the private data. Thus, it is possible to delete the company data at any time without having to access private data. The MDM solution is used for the administration of company mobile phones, as well as for the management of BYOD. In Germany, the second case company has approved BYOD only for a few executives until today. In 2016, the number of requests from employees to use BYOD increased to such an extent that an initiative was launched to use BYOD throughout the entire company. The works council was also consulted. Initially, the German works council expressed concerns over employees' privacy because personal data in the form of employee location could be analyzed by the company. To protect the employee, the works council had considered blocking all location services on smartphones by policy. The IT department pointed out that sales employees in particular need these functions for navigation. Above all, it was made clear that the provider of the MDM solution ensures that no location data can be collected. With these arguments, the data protection concerns of the works council could be alleviated. However, the German works council's concerns about work-life balance and the use of private property for business purposes remained. A voluntary use of the MDM solution is currently only open to executives who are not represented by the German works council. When BYOD is used, the user must agree that the corporate apps are only used for business purposes. In addition, protocol and personal data such as the mobile number or memory usage of the smartphone are recorded on a German server of the MDM provider. However, the company ensures that this data is not used for monitoring or other analyses.

We conclude that employees' privacy concerns play a central role in the BYOD discussion, both for practitioners and academics. The question remains whether the actual users of BYOD, i.e., the employees, share the concerns over privacy expressed by the works councils of the two case companies. We address this question through our survey-based data analysis of employees' privacy concerns.

Hypothesis Development

We build our empirical investigation on the privacy calculus theory (Laufer and Wolfe 1977), which has been widely used in information systems (IS) research (see, e.g., Culnan and Armstrong 1999; Dinev and Hart 2006; Keith et al. 2015; Kordzadeh and Warren 2017; Teubner and Flath 2019). In privacy calculus, individuals assess the degree of privacy they are likely to give up in return for potential benefits, which prompts individuals to perform a risk–benefit analysis of personal information disclosure to assess privacy concerns (Xu et al. 2009). 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" (p. 2). These concerns are related to a "possible loss of privacy as a result of information disclosure" (Xu et al. 2008, p. 4). 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) indicate that difficulties in conflict between private and organizational data occur if employees use their private devices in an organizational context. Through the installation of

MDM software, companies are able to track employees' personal information (PR Newswire 2012). Since privacy concerns are considered to influence an individual's calculation of risk that involves an assessment of the likelihood of negative consequences as well as the perceived severity of those consequences (Smith et al. 2011), we propose the following hypothesis:

H1: Employees' privacy concerns have a significant impact on their perceptions of risks 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" (Smith et al. 2011, p. 1001), 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" (Stone and Stone 1990, p. 363). 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. 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" (p. 320). 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, p. 320). According to several studies, BYOD entails advantages for both employees and companies. For example, a study by Dell (2011) revealed that granting employees more privileges toward a more mobile workplace increases the overall productivity within a company. Moreover, by allowing employees to choose their mobile work devices, their individual efficiency can 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 higher job satisfaction. This is 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:

H2: Employees' perceived risks have a significant impact on the attitude toward using BYOD mobile devices.

H3: Employees' perceived benefits have a significant impact on 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" (Davis et al. 1989, p. 984), which is considered to be the most immediate antecedent of behavioral intention (Fishbein and Ajzen 1975). Ajzen (1991) 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" (p. 181). 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 (see, e.g., Awad and Krishnan 2006; Wu et al. 2012), 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.

H4: Employees' attitude toward using BYOD mobile devices has a significant impact on the intention to use such devices.

Research Design and Results

Data Collection

For our empirical exploration, we designed a survey and distributed it to participants from different countries (United States, Germany, and South Korea) with an online survey (via social networking sites, email, and personal recruitment through professional networking) and written submissions. We have chosen to explore differences among these cultures in order to additionally offer recommendations for

global companies and 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 (Cisco 2013; IDG Connect 2014) and a similar share of mobile phone users (McDermott 2013). 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 owning 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 pre-tests were conducted. The pre-tests 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." 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 of 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). With regard to industry, most German participants were working in IT, while most Korean participants were working in manufacturing. However, the manufacturing sector ranges from handicraft to high-technological manufacturing, thus, IT and smart applications play an increasing role in manufacturing. In order to control for 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 0.14, indicating very low correlations (Hinkle et al. 1988). Thus, 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 version 2.0.M3 (Ringle et al. 2005). SEM provides the ability to model relationships among multiple predictor and multiple criterion variables, which is why SEM is appropriate for analyzing multivariate models (Chin 1998). 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 R^2 and the structural paths (Chin 1998; Gefen et al. 2000; Hair et al. 2017). 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 percent or more of the variance of the underlying LV [latent variable]" (Chin 1998, p. xiii). The measurement items in our model loaded between 0.68 and 0.95 on their respective constructs, thus demonstrating adequate reliability. The internal consistency of the scales was validated with the analysis of Cronbach's alpha ranging from 0.87 to 0.94, and composite reliability (CR) ranging from 0.94 to 0.96. To establish acceptable model reliability, the recommended values for construct reliability are above 0.70 (Gefen et al. 2000); the internal consistency criteria are therefore met. Average variance extracted (AVE) ranged from 0.72 to 0.88, Fornell and Larcker (1981) recommend a lower limit of 0.50 for convergent validity.

In order 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 (Hair et al. 2017). 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 greater than 0.19. Table 1 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, thus, the Fornell-Larcker criterion is met.

Table 1. Correlation Matrix

	PCO	RISK	BEN	ATT	INT
Privacy Concerns (PCO)	**0.85**				
BYOD Risks (RISK)	0.60	**0.92**			
BYOD Benefits (BEN)	−0.05	−0.17	**0.91**		
BYOD Attitude (ATT)	−0.25	−0.42	0.58	**0.89**	
BYOD Intention (INT)	−0.25	−0.39	0.48	0.73	**0.94**

Structural Equation Modeling

The hypotheses were tested by analyzing the structural equation modeling. By looking at the R^2 value, which explains the variance of the respective constructs, the explanatory power of the structural equation modeling can be evaluated. Figure 1 shows the results of the structural equation modeling for the combined data set including all three countries (ALL), and for each country separately.

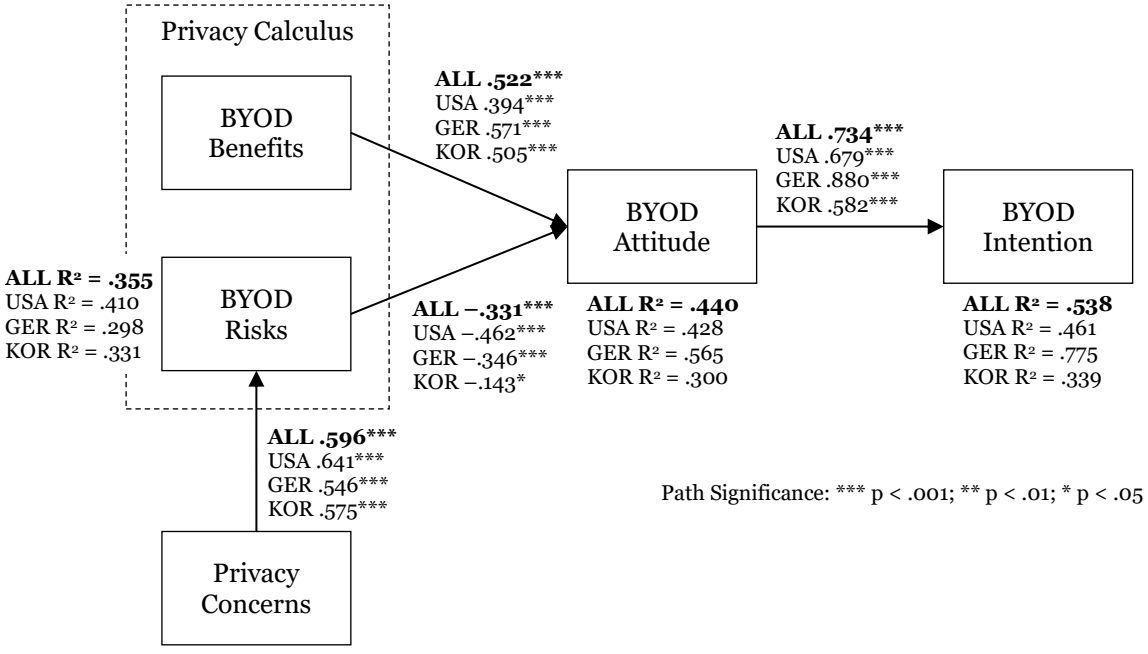

Figure 1. Results of Structural Equation Modeling

Privacy concerns are found to be significantly influencing BYOD risks ($\beta = 0.596$, $p < 0.001$), thus, H1 is supported by our results. BYOD attitude is significantly influenced by BYOD risks ($\beta = -0.331$, $p < 0.001$) and BYOD benefits ($\beta = 0.522$, $p < 0.001$), supporting H2 and H3. Further, BYOD attitude is found to be significantly influencing BYOD intention ($\beta = 0.734$, $p < 0.001$), thus, H4 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. Most interestingly, all three countries have similar

predictive values regarding the influence of privacy concerns on BYOD risks. However, there are substantial differences considering the privacy calculus of the participants from the three countries. While BYOD benefits are more important than BYOD risks to form the attitude of participants from Germany and South Korea, it is the other way round for participants from the United States.

We additionally compared the significance of the path coefficient differences among the three countries using a multi-group analysis of SEM for a statistical test on differences. Results show that the impact of BYOD risks on BYOD attitude is significantly different between the United States and South Korea ($p = 0.001$) as well as between Germany and South Korea ($p = 0.023$). Further, there is a significant difference regarding the impact of BYOD benefits on BYOD attitude between the United States and Germany ($p = 0.019$). Considering the impact of BYOD attitude on BYOD intention, there are significant differences between the United States and Germany ($p = 0.000$) as well as Germany and South Korea ($p = 0.000$). Table 2 shows the results of the multi-group analysis for all relationships of our structural model.

Table 2. Results of Multi-Group Analysis

Path	USA/GER		USA/KOR		GER/KOR	
	Difference	p-value	Difference	p-value	Difference	p-value
PCO --> RISK	0.095	0.110	0.066	0.216	0.029	0.360
RISK --> ATT	0.116	0.099	0.319***	0.001	0.203*	0.023
BEN --> ATT	0.177*	0.019	0.111	0.119	0.066	0.260
ATT --> INT	0.201***	0.000	0.097	0.108	0.298***	0.000

Discussion

Our results reveal that employees share similar privacy concerns to that of the concerns expressed by the works councils from our two case companies. Results of the structural equation modeling show that BYOD risks are largely influenced by employees' privacy concerns ($\beta = 0.596$, $p < 0.001$), which explains 35.5% of the construct's variance. This confirms our assumption from the two case studies that privacy concerns are a barrier for BYOD implementations. However, employees' privacy calculus can be substantially different in diverse cultures; US employees' BYOD risks exceed BYOD benefits, and both German and Korean employees' BYOD benefits exceed risks associated with BYOD. We focus on three representative countries from three different cultures: the United States for the Anglo-American culture, Germany for the Central European culture, and South Korea for the Asian culture. We refer to Hofstede et al.'s (2010) cultural dimensions to derive implications for multinational corporations. Figure 2 shows the culture index for the United States, Germany, and South Korea, based on the six cultural dimensions: power distance, individualism, masculinity, uncertainty avoidance, long-term orientation, and indulgence.

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. (2010), 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" (Hofstede et al. 2010, p. 92). 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 while privacy concerns have similar effects on BYOD risks across different cultures, the privacy calculus diverts substantially: the predictive value of BYOD risks to explain the attitude towards BYOD is larger for highly individualist cultures such as the United States ($\beta = -0.462$, $p < 0.001$) compared to Germany ($\beta = -0.346$, $p < 0.001$) and to a highly collectivist culture like South Korea ($\beta = -0.143$, $p < 0.05$). 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

(Hsee and Weber 1999). Since the cultural dimension of uncertainty avoidance refers to a reduction of ambiguity instead of reducing risk (Hofstede et al. 2010), 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. As expressed by the works councils of our case companies, work-life balance is another risk induced by BYOD. Since our focus is on BYOD privacy, we omitted BYOD work-life balance research, which has been in the focus of other IS studies (see, e.g., Al Askar and Shen 2016; Köffer et al. 2014; Qi et al. 2017). However, we note that several cultural dimensions including masculinity, uncertainty avoidance, long-term orientation, and indulgence have an influence on work-life balance, which affect BYOD benefits and risks. Further research is needed to investigate the interrelation between cultural differences and BYOD work-life balance to advance knowledge on BYOD diffusion.

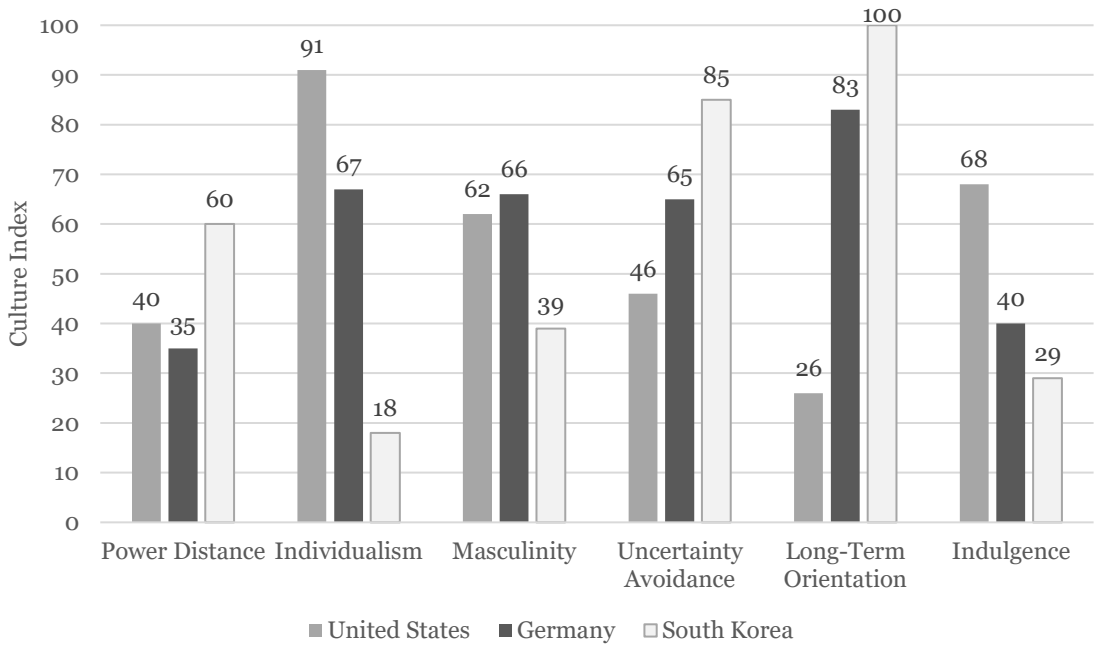

Figure 2. Cultural Dimensions (United States, Germany, and South Korea)

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 (Hofstede et al. 2010). 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" (Hofstede et al. 2010, p. 61). In our study, employees' attitude towards BYOD from Germany as a small power distance culture (culture index: 35) has the highest impact on BYOD intention ($\beta = 0.880$, $p < 0.001$), explaining 77.5% of the construct's variance, followed by employees from the United States (power distance culture index: 40), whose attitude towards BYOD has the second-highest impact on BYOD intention ($\beta = 0.679$, $p < 0.001$), explaining 46.1% of the construct's variance, and employees from South Korea as a large power distance culture (60), whose BYOD attitude has the lowest impact on BYOD intention ($\beta = 0.582$, $p < 0.001$), explaining only 33.9% of the construct's variance. For future BYOD studies, which do not have a focus neither on BYOD privacy nor on BYOD work-life balance, but focus on BYOD adoption and cultural differences from an employee compliance perspective, we recommend an investigation on what other factors could influence BYOD intention, given the rather small R^2 value of 0.339 for Korean employees compared to that of their American and German counterparts.

Since cultural dimensions and cultural scores of the countries are viewed as a point of reference in the domestic population of a country (Jones and Alony 2007), we additionally found implications from an organizational culture perspective, because organizational cultures are different in many respects from national cultures (Hofstede et al. 2010). As Allen et al. (2007) 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 (Chang et al. 2015). Our two cases show that employers are setting up policies and works council agreements to influence their employees' perception of a company's privacy rules. Such agreements between employee and employer are positively associated with reducing concerns, if they meet employee expectations and provide a secure feeling for the employees (Chang et al. 2015). We recommend that further research 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. In our survey, we have asked respondents about the information sensitivity of corporate data and the permission to use BYOD mobile devices, which provides initial indications through an additional analysis of the structural model relations. While the sensitivity of corporate data has no significant impact on employees' privacy concerns ($\beta = 0.021$, $p > 0.05$), the permission to use BYOD mobile devices shows a significant influence on privacy concerns ($\beta = 0.145$, $p < 0.001$). We suggest that further research analyzes the impact of the sensitivity of personal information on privacy concerns in order to gain deeper insights on what type of information needs to be safeguarded to protect employees' privacy when implementing BYOD into an organization. We further recommend that the permission to use BYOD mobile devices requires a more in-depth analysis. When employees are using their private IT without explicit approval or even knowledge of the company (Haag and Eckhardt 2017), this provides additional implications for the introduction of BYOD and associated concerns for information privacy.

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. For instance, the European Union (EU) has implemented the General Data Protection Regulation (GDPR) requiring measures to protect EU citizens (Nadeau 2018). In the United States, the California Consumer Privacy Act (CCPA) has been passed in June 2018, mirroring the EU's GDPR (Stanberry 2018). The CCPA is scheduled to become effective on January 1, 2020. Nevada, New York, and Washington, DC followed California's CCPA (Serrato and Ross 2019). 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. 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 GDPR and CCPA to avoid any legal complications through the implementation of BYOD. Further research can investigate whether regulatory initiatives, such as 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.

Our first limitation relates to the sample used here, as it consists of American, German, and Korean employees. Consequently, we only discuss differences in these three cultures. Leidner and Kayworth (2006) showed that national culture significantly impacts IS studies. Our results can only be generalized to other cultures with caution. In addition, we acknowledge that interdependencies between the multiple layers of culture exist, e.g., national layer, organizational layer, subunit layer or professional layer (Guhr et al. 2018; Leidner and Kayworth 2006). We further acknowledge that we interpret cultural differences by referring to Hofstede et al.'s 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 (Tang and Koveos 2008), we do not assume that the cultural dimensions have changed substantially over time. In terms of generalizability, the second limitation refers to a bias possibility of self-selection among the survey respondents (Kankanhalli et al. 2005). 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. The third limitation is regarding our assumption that works councils are concerned with the privacy of employees, on which we build our research on employees' privacy concerns for BYOD implementations. The generalizability of this

assumption is limited due to the selection of two case companies and the interpretive nature of the case studies. However, we ensured to select real-world case companies, in which the implementation of BYOD has actually been extensively discussed with works councils and de facto implemented into both companies. While we think that other companies may have expressed similar concerns about employees' privacy, we cannot rule out that other companies and organizations used different BYOD implementations, or even rejected to implement BYOD. Since both our case companies are headquartered in Germany, but operate across multiple countries, we recommend further research looking at companies headquartered in other countries and at companies that rejected the implementation of BYOD.

Conclusions and Outlook

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 companies and organizations. In IT consumerization, BYOD combines private ownership and organizational use. Several benefits and challenges for both employees and companies arise. With regard to our first research question, we presented insights from two multinational case companies, where works councils have expressed their concerns with privacy intrusion into employees' lives through BYOD. Regarding the second research question, we 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, e.g., that American employees place greater emphasis on BYOD risks associated with privacy concerns compared to employees from Germany and South Korea. Due to the growing "anytime, anywhere" mindset 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 in order 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 companies and organizations to face the growing pressure to integrate BYOD.

Acknowledgements

The authors acknowledge Professors Namyong Lee (Soongsil University); Jongki Kim (Pusan National University); Joon Koh (Chonnam National University); and other Korean IT professionals who collected survey data from participants in South Korea. We thank all the participants from the United States, Germany, and South Korea for participating in our study. We are indebted to the associate editor and the four anonymous reviewers for their constructive feedback and valuable suggestions. We are also grateful to Jan Recker and Maura Atapattu for their valuable feedback on an earlier version of the paper. We thank Benedikt Lebek for his contributions to preliminary findings from this study, which were presented at the 19th Americas Conference on Information Systems.

References

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

Al Askar, M., and Shen, K. N. 2016. "Understanding Bring Your Own Device (BYOD) and Employee Information Security Behaviors from a Work-Life Domain Perspective," in *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego, CA, August 11-13, pp. 1-10.

Allen, M. W., Coopman, S. J., Hart, J. L., and Walker, K. L. 2007. "Workplace Surveillance and Managing Privacy Boundaries," *Management Communication Quarterly* (21:2), pp. 172-200.

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization," *MIS Quarterly* (30:1), pp. 13-28.

Bygstad, B. 2017. "Generative Innovation: A Comparison of Lightweight and Heavyweight IT," *Journal of Information Technology* (32:2), pp. 180-193.

Chang, S. E., Liu, A. Y., and Lin, S. 2015. "Exploring Privacy and Trust for Employee Monitoring," *Industrial Management & Data Systems* (115:1), pp. 88-106.

Chin, W. W. 1998. "Issues and Opinion on Structural Equation Modeling," *MIS Quarterly* (22:1), pp. vii-xvi.

Cisco. 2013. "The Financial Impact of BYOD: A Model of BYOD's Benefits to Global Companies," from http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD-Economics_Presentation.pdf

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

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

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), pp. 982-1003.

Dell. 2011. "The Evolving Workforce: How Was Work Today? New Study Reveals Workforce Trends of Today and the Future," from http://content.dell.com/us/en/corp/d/corp-comm/the-evolving-workforce/

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Eze Castle Integration. 2018. "Developing a BYOD or MDM Policy for Your Firm," from https://www.eci.com/blog/439-developing-a-byod-or-mdm-policy-for-your-firm.html

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

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

French, A. M., Guo, C. J., and Shim, J. P. 2014. "Current Status, Issues, and Future of Bring Your Own Device (BYOD)," *Communications of the Association for Information Systems* (35), pp. 191-197.

Gefen, D., Straub, D. W., and Boudreau, M.-C. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the Association for Information Systems* (4:7), pp. 1-77.

Guhr, N., Nolte, F., and Breitner, M. H. 2018. "Enterprise Professional Diversity and Challenges for Social-Collaboration Technologies," *International Journal of Business and Social Science* (9:1), pp. 39-50.

Haag, S., and Eckhardt, A. 2017. "Shadow IT," *Business & Information Systems Engineering* (59:6), pp. 469-473.

Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2017. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks, CA: Sage Publications.

Hinkle, D. E., Wiersma, W., and Jurs, S. G. 1988. *Applied Statistics for the Behavioral Sciences*, (2nd ed.). Boston, MA: Houghton Mifflin Company.

Hofstede, G., Hofstede, G. J., and Minkov, M. 2010. *Cultures and Organizations: Software of the Mind – Intercultural Cooperation and Its Importance for Survival*, (3rd ed.). New York: McGraw-Hill.

Hsee, C. K., and Weber, E. U. 1999. "Cross-National Differences in Risk Preference and Lay Predictions," *Journal of Behavioral Decision Making* (12:2), pp. 165-179.

IDG Connect. 2014. "South Korea: BYOD Spotlight," Framingham, MA.

Johnson, N., and Joshi, K. D. 2012. "The Pathway to Enterprise Mobile Readiness: Analysis of Perceptions, Pressures, Preparedness, and Progression," in *Proceedings of the 18th Americas Conference on Information Systems*, Seattle, WA, August 9-12, pp. 1-8.

Jones, M., and Alony, I. 2007. "The Cultural Impact of Information Systems – Through the Eyes of Hofstede – A Critical Journey," *Issues in Informing Science and Information Technology* (4:1), pp. 407-419.

Junglas, I., Goel, L., Ives, B., and Harris, J. 2019. "Innovation at Work: The Relative Advantage of Using Consumer IT in the Workplace," *Information Systems Journal* (29:2), pp. 317-339.

Kankanhalli, A., Tan, B. C. Y., and Wei, K.-K. 2005. "Contributing Knowledge to Electronic Knowledge Repositories: An Empirical Investigation," *MIS Quarterly* (29:1), pp. 113-143.

Karanasios, S., and Allen, D. 2014. "Mobile Technology in Mobile Work: Contradictions and Congruencies in Activity," *European Journal of Information Systems* (23:5), pp. 529-542.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., and Abdullat, A. 2015. "The Role of Mobile-Computing Self-Efficacy in Consumer Information Disclosure," *Information Systems Journal* (25:6), pp. 637-667.

Kim, D., Park, K., Park, Y., and Ahn, J.-H. 2019. "Willingness to Provide Personal Information: Perspective of Privacy Calculus in IoT Services," *Computers in Human Behavior* (92), pp. 273-281.

Köffer, S., Junglas, I., Chiperi, C., and Niehaves, B. 2014. "Dual Use of Mobile IT and Work-to-Life Conflict in the Context of IT Consumerization," in *Proceedings of the 35th International Conference on Information Systems*, Auckland, New Zealand, December 14-17, pp. 1-19.

Köffer, S., Ortbach, K., Junglas, I., Niehaves, B., and Harris, J. 2015. "Innovation through BYOD? The Influence of IT Consumerization on Individual IT Innovation Behavior," *Business & Information Systems Engineering* (57:6), pp. 363-375.

Kordzadeh, N., and Warren, J. 2017. "Communicating Personal Health Information in Virtual Health Communities: An Integration of Privacy Calculus Model and Affective Commitment," *Journal of the Association for Information Systems* (18:1), pp. 45-81.

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues* (33:3), pp. 22-42.

Lee Jr., J., Crossler, R. E., and Warkentin, M. 2013. "Implications of Monitoring Mechanisms on Bring Your Own Device (BYOD) Adoption," in *Proceedings of the 34th International Conference on Information Systems*, Milan, Italy, December 15-18, pp. 1-12.

Leidner, D. E., 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.

Loose, M., Weeger, A., and Gewald, H. 2013. "BYOD – The Next Big Thing in Recruiting? Examining the Determinants of BYOD Service Adoption Behavior from the Perspective of Future Employees," in *Proceedings of the 19th Americas Conference on Information Systems*, Chicago, IL, August 15-17, pp. 1-12.

MarketsandMarkets. 2016. "BYOD & Enterprise Mobility Market Worth 73.30 Billion USD by 2021," from https://www.marketsandmarkets.com/PressReleases/byod.asp

McDermott, J. 2013. "A Majority of U.S. Mobile Users Are Now Smartphone Users," from http://adage.com/article/digital/a-majority-u-s-mobile-users-smartphone-users/241717

Meeker, M. 2015. "Internet Trends 2015," from https://www.kleinerperkins.com/internet-trends/

Middleton, C., Scheepers, R., and Tuunainen, V. K. 2014. "When Mobile Is the Norm: Researching Mobile Information Systems and Mobility as Post-Adoption Phenomena," *European Journal of Information Systems* (23:5), pp. 503-512.

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

Minch, R. P. 2004. "Privacy Issues in Location-Aware Mobile Devices," in *Proceedings of the 37th Hawaii International Conference on System Sciences*, Waikoloa, HI, January 5-8, pp. 1-10.

Nadeau, M. 2018. "General Data Protection Regulation (GDPR): What You Need to Know to Stay Compliant," from https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

Niehaves, B., Köffer, S., and Ortbach, K. 2012. "IT Consumerization – A Theory and Practice Review," in *Proceedings of the 18th Americas Conference on Information Systems*, Seattle, WA, August 9-12, pp. 1-9.

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), pp. 330-346.

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), pp. 324-340.

Ortbach, K., Walter, N., and Öksüz, A. 2015. "Are You Ready to Lose Control? A Theory on the Role of Trust and Risk Perception on Bring-Your-Own-Device Policy and Information System Service Quality," in *Proceedings of the 23rd European Conference on Information Systems*, Münster, Germany, May 26-29, pp. 1-10.

Osterman Research. 2012. "Putting IT Back in Control of BYOD," Black Diamond, WA.

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), pp. 105-136.

Picoto, W. N., Bélanger, F., and Palma-dos-Reis, A. 2014. "An Organizational Perspective on M-Business: Usage Factors and Value Determination," *European Journal of Information Systems* (23:5), pp. 571-592.

PR Newswire. 2012. "Harris Survey Exposes Concerns About Employee Privacy for BYOD," from http://www.prnewswire.com/news-releases/harris-survey-exposes-concerns-about-employee-privacy-for-byod-171520251.html

Putri, F., and Hovav, A. 2014. "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory," in *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv, Israel, June 9-11, pp. 1-17.

Qi, C., Huang, J., and Liu, O. 2017. "Exploring the Antecedents of Work-to-Life Conflict under the Context of Bring Your Own Device," in *Proceedings of the 21st Pacific Asia Conference on Information Systems*, Langkawi, Malaysia, July 16-20, pp. 1-6.

Ringle, C. M., Wende, S., and Will, A. 2005. "SmartPLS 2.0.M3," from http://www.smartpls.com

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

Saha, D., and Mukherjee, A. 2003. "Pervasive Computing: A Paradigm for the 21st Century," *Computer* (36:3), pp. 25-31.

Schmitz, K. W., Teng, J. T. C., and Webb, K. J. 2016. "Capturing the Complexity of Malleable IT Use: Adaptive Structuration Theory for Individuals," *MIS Quarterly* (40:3), pp. 663-686.

Serrato, J. K., and Ross, S. 2019. "Nevada, New York and Other States Follow California's CCPA," from https://www.dataprotectionreport.com/2019/06/nevada-new-york-and-other-states-follow-californias-ccpa/

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp. 989-1015.

Sørensen, C., and Landau, J. S. 2015. "Academic Agility in Digital Innovation Research: The Case of Mobile ICT Publications within Information Systems 2000-2014," *Journal of Strategic Information Systems* (24:3), pp. 158-170.

Spagnoletti, P., Resca, A., and Sæbø, Ø. 2015. "Design for Social Media Engagement: Insights from Elderly Care Assistance," *Journal of Strategic Information Systems* (24:2), pp. 128-145.

Stanberry, R. 2018. "California Consumer Privacy Act of 2020 (CCPA)," from https://medium.com/@rustystanberry/california-consumer-privacy-act-of-2018-ccpa-f9d09fb303fc

Steelman, Z. R., Lacity, M., and Sabherwal, R. 2016. "Charting Your Organization's Bring-Your-Own-Device Voyage," *MIS Quarterly Executive* (15:2), pp. 85-104.

Steinbart, P. J., Keith, M. J., and Babb, J. 2016. "Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication," *Information Systems Research* (27:2), pp. 219-239.

Stone, E. F., and Stone, D. L. 1990. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8:3), pp. 349-411.

Tang, L., and Koveos, P. E. 2008. "A Framework to Update Hofstede's Cultural Value Indices: Economic Dynamics and Institutional Stability," *Journal of International Business Studies* (39:6), pp. 1045-1063.

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

Teubner, T., and Flath, C. M. 2019. "Privacy in the Sharing Economy," *Journal of the Association for Information Systems* (20:3), pp. 213-242.

Tu, Z., and Yuan, Y. 2015. "Coping with BYOD Security Threat: From Management Perspective," in *Proceedings of the 21st Americas Conference on Information Systems*, Puerto Rico, August 13-15, pp. 1-6.

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

Warkentin, M., Walden, E., Johnston, A. C., and Straub, D. W. 2016. "Neural Correlates of Protection Motivation for Secure IT Behaviors: An Fmri Examination," *Journal of the Association for Information Systems* (17:3), pp. 194-215.

Wottrich, V. M., van Reijmersdal, E. A., and Smit, E. G. 2018. "The Privacy Trade-Off for Mobile App Downloads: The Roles of App Value, Intrusiveness, and Privacy Concerns," *Decision Support Systems* (106), pp. 44-52.

Wu, K.-W., Huang, S. Y., Yen, D. C., and Popova, I. 2012. "The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust," *Computers in Human Behavior* (28:3), pp. 889-897.

Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," in *Proceedings of the 29th International Conference on Information Systems*, Paris, France, December 14-17.

Xu, H., Teo, H.-H., Tan, B. C. Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-173.

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., and Zhu, Q. 2018. "Health Information Privacy Concerns, Antecedents, and Information Disclosure Intention in Online Health Communities," *Information & Management* (55:4), pp. 482-493.

Appendix

Table A1. Survey Instrument

Items	English	German	Korean
Privacy Concerns (PCO), Source: Pavlou et al. (2007)			
	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)…
PCO1	I would be concerned that my employer is collecting too much information about me, for example, profiles of social networks, private emails, 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 이멜, 사진, 소셜넷워크등에 관한 정보수집을 하리라 걱정된다.
PCO2	I would be concerned about my privacy.	wäre ich über meine Privatsphäre besorgt.	나의 비밀(프라이버시)에 걱정된다.
PCO3	my personal information could be misused.	könnten meine persönlichen Informationen missbraucht werden.	나의 개인정보가 오용되리라 생각한다.
PCO4	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.
PCO5	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 개인자료를 스캔할수도 있음에 괴롭히게 한다.
PCO6	my personal information could be accessed by unknown parties.	könnten sich unbekannte Dritte Zugang zu meinen persönlichen Informationen verschaffen.	나의 개인정보가 모르는 삼자에게 접근될수도 있다.
BYOD Risks (RISK), Source: Pavlou et al. (2007)			
	I believe that using my private mobile device for work purposes would…	Ich denke, dass die Nutzung meines privaten mobilen Endgeräts für berufliche Zwecke…	직무를 하는데, 나의 개인 모바일 기기를 사용함이…
RISK1	involve a high degree of uncertainty (private and/or work related).	einen hohen Grad an Unsicherheit mit sich bringen würde (privat und/oder beruflich).	직무와 개인일로써, 고도의 불확실성이 있다고 본다.
RISK2	fill me with concerns (private and/or work related).	mich im Allgemeinen mit Sorge erfüllen würde (privat und/oder beruflich).	직무와 개인일로써, 걱정이 된다.
RISK3	be questionable (private and/or work related).	bedenklich wäre (privat und/oder beruflich).	직무와 개인일로써, 의심이 된다.
RISK4	expose me to many uncertainties (private and/or work related).	mich vielen Unsicherheiten aussetzen würde (privat und/oder beruflich).	직무와 개인일로써, 불확실성이 개연된다.
BYOD Benefits (BEN), Source: Davis (1989)			
	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 생산성를 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. (2005); Taylor and Todd (1995)			
	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 Davis (1996); Oliver and Bearden (1985)			
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 company (# 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 company								
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%
Do you have the permission by your company to use your private mobile device for work purposes?								
Yes	114	54.3%	56	31.5%	74	48.1%	244	45.0%
No	78	37.1%	104	58.4%	80	51.9%	262	48.3%
Not specified	18	8.6%	18	10.1%	0	0.0%	36	6.6%