Employee Acceptance of Employer Control Over Personal Devices – Research in Progress

Kevin Callies  
_Dakota State University_, krcallies@dsu.edu

Cherie Bakker Noteboom  
_Dakota State University_, cherie.noteboom@dsu.edu

Daniel Talley  
_Dakota State University_, daniel.talley@dsu.edu

Yong Wang  
_Dakota State University_, yong.wang@dsu.edu

Follow this and additional works at: [https://aisel.aisnet.org/mwais2019](https://aisel.aisnet.org/mwais2019)
Employee Acceptance of Employer Control Over Personal Devices – Research in Progress

Kevin Callies  
Dakota State University  
kcailles@dsu.edu

Cherie Noteboom  
Dakota State University  
cherie.noteboom@dsu.edu

Daniel Talley  
Dakota State University  
daniel.talley@dsu.edu

Yong Wang  
Dakota State University  
yong.wang@dsu.edu

ABSTRACT
Organizations face new and growing security challenges as consumer technology continues to be integrated into organizational workflows. Bring your own device (BYOD) is a phenomenon that is here to stay; however, securing employee's personally-owned devices may require the organizations to consider exerting some control over the employee’s device. In order for organizations to secure access to their sensitive information in this way, they must first garner the employee’s consent. This research seeks to model employee acceptance of employer control by constructing a model of employee acceptance based upon the extant acceptance literature. Future research can test the model by operationalizing the proposed constructs and applying a quantitative survey methodology. The results from this research could potentially aid in the development of future BYOD security measures and help employers develop effective strategies for implementing BYOD security.

Keywords
Technology acceptance, BYOD, Policy acceptance, Unified theory of acceptance and use of technology (UTAUT), UTAUT2

INTRODUCTION
Employees are increasingly demanding to be allowed to use their own personal devices, or other consumer technology, for work-related tasks even if it goes against an organization’s current security policy (Dillow, 2013; Eddy, 2013). When companies allow employees to use personal devices for a work-related task it is typically referred to as Bring Your Own Device or BYOD for short. The use of personal devices for work activities opens up a whole new arena of security and privacy concerns (Miller, Voas, & Hurlburt, 2012). Several solutions have been proposed for the organizational concern of privacy, including exerting some control over the employee’s privately-owned device (French, Guo, & Shim, 2014). These solutions include employees installing special applications or device management software to maintain control over the organization’s sensitive data. A key aspect of this security paradigm is the employee’s consent. This research proposes to adapt the Unified Theory of Acceptance and Use of Technology (UTAUT) and its extension as a model for employee acceptance of employer control over their personally-owned devices.

While the prior research into technology acceptance provides an appropriate starting point for the development of a model of employee acceptance, it has not been applied or empirically tested in the same manner as suggested by this research. In the end there are two primary goals for this research. First, this research seeks to examine the factors that support employee acceptance of employer control over personally-owned devices. Second, this research seeks to expand and support the existing technology acceptance literature by moving it into a new domain.

Modeling employee acceptance of employer control can identify the most important factors for ensuring employee compliance with required BYOD security measures. By examining the factors that may affect employee acceptance employers can ensure they are applying the most effective means of securing personal devices given the rapid expansion of consumer technology in the workplace. Further testing of the model can provide empirical evidence showing which factors are most significant when it comes to affecting employee behavior. With these results organizations can choose the best methods for enforcing BYOD security and implementing policies. Researchers can also benefit from the empirical demonstration of this model as it provides another test of the extant technology acceptance literature and can help direct future BYOD security and policy research.
THEORETICAL BACKGROUND

BYOD is here and appears to be on the rise (Eddy, 2013); therefore, organizations must address the security and privacy concerns that accompany BYOD. Author Scarfo summarized the BYOD security approaches as “…two opposite approaches: hands-off devices versus hands-on devices.” (2012, p. 451). There are certain benefits to a hands-on approach to BYOD security such as quicker response times and less network dependence; additionally, end users tend to prefer native applications (Abed, 2016; Forrester, 2015). This means that one of the two major approaches to security in BYOD requires the employer to apply some control over the employee’s device. However, employees must accept the hands-on approach as the organization will need access to their personal devices in order to install the device management applications. Employee consent to employer control of their personal devices has yet to be fully researched, but there are several IT behavior models that can be used as the theoretical background for predicting employee behavior.

The Unified Theory of Acceptance and Use of Technology (UTAUT) as proposed by Venkatesh, Morris, Davis, and Davis (2003) attempts to build upon and synthesize other models including the influential technology acceptance model (TAM). TAM has been used and applied in a variety of contexts since its inception in 1989 (Davis, Bagozzi, & Warshaw, 1989) and has seen several extensions including TAM2 (Venkatesh & Davis, 2000) and more recently UTAUT. Similarly, UTAUT has been extended with the addition of several new constructs in a model known as UTAUT2 (Venkatesh, Thong, & Xu, 2012). The original UTAUT model distills several different acceptance models into four main constructs that are theorized as antecedents of technology acceptance intentions, which subsequently predicts actual behavior. These antecedents include performance expectancy, effort expectancy, social influence, and facilitating conditions. UTAUT2 extended the original model by adding hedonic motivation, price value, and habit again theorizing these new constructs as influencing behavior intentions. The application of UTAUT has been found fairly consistent and is a good place to start for modeling user acceptance of employer control.

MODEL DEVELOPMENT

Most research has used a combination of variables and constructs from the prevailing social theories in a similar manner as presented in this research. This suggests that extending and applying either TAM and its extensions into acceptance of employer control is appropriate. The relevant constructs that can be adapted to an employee’s acceptance of their employer exercising control over their personally owned device are: performance expectancy, effort expectancy, social influence, facilitating conditions, habit, and price.

Performance expectancy, is the employee’s subjective view of how much a technology will enhance their job performance. Effort expectancy is adapted to this research as an employee’s perceived effort required to incorporate BYOD into their everyday work. The construct of social influence attempts to encapsulate the peer pressure an individual may feel to conform to a particular action, in this case the acceptance of employer control. Facilitating conditions is considered the employee’s view of the BYOD technical and managerial support they will receive while complying with the employer’s control. Habit is defined as the employee’s prior capitulation to employer control and their tendency to perform behaviors automatically. The final construct, price value, is the individual’s subjective value of the new technology compared to its associated monetary costs.

These constructs are included in the UTAUT2 model of employee acceptance but have yet to be applied in the same context as this research. Each relationship between the aforementioned constructs and employee acceptance intentions forms the basis for each hypothesis proposed by this research. These hypotheses and the associated relationships are summarized in the path model shown in Figure 1.
FUTURE METHODOLOGY

The model posits six constructs that directly affect an employee’s acceptance intentions. To measure the constructs hypothesized in this research, a survey instrument can be created based upon measures used in other technology acceptance research. Meaning, each construct is operationalized by examining other research that includes similar constructs and adapting the measures to this research. The measures will assess employee beliefs and can be administered via survey. Once data has been collected the model can be empirically examined through structural equation modeling, using a two-step approach (Anderson & Gerbing, 1988). A two-step approach would first validate the measures to ensure they sufficiently capture the desired constructs then apply further analysis to estimate the relationships between the latent constructs.

EXPECTED RESULTS

If the model proves successful in predicting employee acceptance it would be meaningful for practitioners, developers, and other BYOD researchers. This research could be used by organizational leaders when creating their own BYOD policies or implementing their chosen security solutions. If organizations wish to apply control over devices for security or privacy reasons, they would be able to use the significant constructs from this study to ensure acceptance. Developers of security software applications and mobile management software could also utilize this research to instruct their creation of software security solutions. Meaning managers can attempt to influence the hypothesized antecedents to ensure acceptance and developers can continue to develop employer-controlled software applications. Additionally, employees can suggest employers provide the necessary conditions to make employer control more agreeable.

While unexpected the opposite outcome could provide useful insight to other researchers. The acceptance theories on which this model is based are generally well respected and a negative outcome would mean that new constructs may be needed to explain employee acceptance of control. This would require more research and possibly the introduction of brand-new models or antecedents.

REFERENCES


