View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

DIGIT 2014 Proceedings

Diffusion Interest Group In Information Technology

12-14-2014

IT Consumerization: A Model of Private IT Use in Organizations

Naqaash Pirani
Ivey Business School, npirani@ivey.ca

Darren Meister
Ivey Business School, dmeister@ivey.ca

Follow this and additional works at: http://aisel.aisnet.org/digit2014

Recommended Citation

Pirani, Naqaash and Meister, Darren, "IT Consumerization: A Model of Private IT Use in Organizations" (2014). *DIGIT 2014 Proceedings*. 5.
http://aisel.aisnet.org/digit2014/5

This material is brought to you by the Diffusion Interest Group In Information Technology at AIS Electronic Library (AISeL). It has been accepted for inclusion in DIGIT 2014 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

IT Consumerization: A Model of Private IT Use in Organizations

Research-in-Progress

Naqaash Pirani
Ivey Business School
Western University
1255 Western Road
London, Ontario, Canada
npirani@ivey.ca

Darren Meister
Ivey Business School
Western University
1255 Western Road
London, Ontario, Canada
dmeister@ivey.ca

Abstract

IT Consumerization, the use of privately-owned IT devices and applications in place of business IT, has become a significant trend in organizations today. We provide a review and interpretation of existing literature on IT Consumerization, incorporating research on boundary blurring, bring-your-own-device (BYOD) programs and Shadow IT. We then synthesize and extend the current body of knowledge by drawing on general deterrence theory, expectation-confirmation theory and neutralization theory to provide a model of private IT use within the enterprise. Our aim is to contribute to an understanding of the paths by which various categories of private IT use occur, and develop a testable research model to allow them to be explored in a coherent manner.

Keywords: IT Consumerization, Boundary Blurring, BYOD, Shadow IT

Introduction

IT Consumerization is the macro phenomenon in which devices and applications that originate in the consumer market are used in addition to, or in lieu of, business IT (Harris et al. 2012; Ortbach et al. 2013). The Apple iPhone and iPad are prime examples of technologies that were considered and adopted as part of the consumer market well before being considered as core to the enterprise contexts. According to a global survey by Accenture in 2011, 23% of employees are now using personal technology tools like the iPhone or iPad for work on a routine basis (Harris et al. 2012). Seen from this perspective, the traditional direction of technology is shifting from enterprise-drive phenomenon to a to a consumer-driven one (Niehaves et al. 2012).

Our aim in this paper is to extend prior research on IT Consumerization by developing a model of private IT use within organizations. Private IT use encompasses the different ways in which employee-owned devices and applications are used within a work setting. We choose to focus specifically on mobile technology use, which we define as the use of portable IT devices including laptops, smartphones and tablets. Drawing on existing studies of IT Consumerization (Niehaves et al. 2012; Schalow et al. 2013), the four categories of private IT use that can occur within an organization are: no private IT use (Px), private IT use for private purposes (Pp), unauthorized use of private IT for business purposes (UAPb) and the authorized use of private IT for business purposes (APb). Understanding how and why paths towards these different categories of private IT use evolve is of significant importance for academics and practitioners as each can lead to different outcomes for the focal organization. For example, the unauthorized use of private IT for business purposes is part of what is often referred to as Shadow IT, a form behaviour that is not compliant with organizational information security policies (Györy et al. 2012). This is a concern for the organization as it places IT use outside of their monitoring abilities and may thus lead to an increase in IT-related incidents, such as intellectual property loss or theft. On the other hand, authorized use of private IT for business purposes may be beneficial to organizations as private IT is often seen by employees as being more powerful and useful, as well as easier and more fun to use, than traditional business IT (Harris et al. 2012).

The paper is organized as follows: In the first section, we define the various categories of private IT use and highlight the precursors and triggers that have been identified in previous IT Consumerization research. In the next section, we propose a model of private IT use in organizations that builds on prior work and incorporates general deterrence theory (Gibbs 1975), expectation-confirmation theory (Oliver 1980) and neutralization theory (Sykes and Matza 1957) to complete the missing links. In the third and final section, we begin to theorize around the paths that can lead to different categories of private IT use and how these may impact an organization and its employees. We conclude with a discussion of next steps and our expected contributions.

Related Literature

This section first begins with a definition of the various categories of private IT use in organizations and then highlights the precursors and triggers for the different categories that have been identified in previous IT Consumerization literature.

Categories of IT Use in Organizations

We can identify four different categories of IT use in organizations based on the ownership of the technology (business vs. private) and the purpose to which it is applied (business vs. private) (See Figure 1). When business IT is used by employees for business purposes or private purposes, employees have not yet provisioned their own devices into the workplace and so we label this category “no private IT use” (Px)[1]. This was the status quo before the trend towards IT Consumerization began, and may still exist in organizations today where highly sensitive or confidential information is being handled (e.g. Government, Health Care, Financial Services). However, when private IT are used by employees within an organization for private purposes (Pp) the employee has provisioned their own device(s) in the workplace, and may or

[1] This category may encompass a wide range of uses, but since our focus is on Private IT use rather than Business IT use, we have chosen not to explore it further

may not be acting in a manner that is in accordance with the information security policies (ISPs) of the organization. ISPs define the roles and responsibilities of employees to safeguard the information and technology resources of the their organizations (Bulgurcu et al. 2010) and terms like "IT misuse" and "IT abuse" are used to describe instances where activity is in violation of them (Schalow et al. 2013).

The use of private IT by employees for business purposes is what is often captured under the umbrella of "IT Consumerization" (Harris et al. 2012; Niehaves et al. 2012). Within this category of technology use, there are two distinct sub-categories that can be identified. When the use of private IT for business purposes is supported by the organization, this can be referred to as "authorized use of private IT for business purposes" (APb). Bring-your-own-device (BYOD) programs, in which employees are encouraged to purchase their own IT devices and use them for business purposes, are a prime example of such authorized use. On the other hand, if the use of private IT for business purposes is *not* supported by the organization (as indicated by their ISP), this falls under the sub-category of "unauthorized use of private IT for business purposes" (UAPb). It is worth nothing that while such use is not authorized by an organization, it may still be in line with the features and spirit of the private IT itself. Therefore, it does not represent an unfaithful appropriation as defined by DeSanctis and Poole (1994), and cannot be represented using Adaptive Structuration Theory.

Instead, the unauthorized use of private IT for business purposes has been discussed in IT Consumerization literature as "Shadow IT," a form of non-IT Security compliant behaviour that can pose a significant risk to organizations (Győry et al. 2012). For example, when individuals provision their own mobile devices into the workplace and use them for unauthorized business purposes (such as accessing corporate email without permissions), the organization may be placed at an increased risk of intellectual property loss or theft. When a business-owned mobile device is reported lost or stolen, corporate IT has the ability to remotely wipe the device of any sensitive information. However, when an employee-owned device is lost, these safeguards are of little help. Similarly, if an employee chooses to use a personal laptop or tablet for a business activity (creating a report, for example) and then takes that device home with them, there is a risk that the information could be accessed by unauthorized parties by taking advantage of the employee's less-secure home wireless network.

		Purpose	
		Private	**Business**
Ownership	**Private**	Private IT for Private Purposes (Pp) – IT Misuse/Abuse	Unauthorized use of Private IT for Business Purposes (UAPb) – Shadow IT
			Authorized use of Private IT for Business Purposes (APb) – e.g. BYOD
Ownership	**Business**	No Private IT use (Px)	

Figure 1 – Categories of IT use in organizations

Preconditions and Triggers for Categories of IT use

IS researchers have begun to explore the preconditions and triggers that lead to different forms of private IT use in organizations, what they term "Boundary Blurring" behaviour (Schalow et al. 2013)[2]. The four states they focus on are; the use of private IT for private purposes (Pp), the unauthorized use of private IT

[2] In Schalow et al. 2013, the phenomenon of interest is media use, not IT use. For consistency, we refer to this as IT use throughout the paper.

for business purposes (UAPb), the authorized use of private IT for business purposes (APb) and the use of private IT for teleworking (not in the scope of this paper)[3]. In the resulting model, own resource provision (ORP), that is, bringing one's own devices or IT into the workplace, is a precondition of all categories of boundary-blurring behaviour. This is not surprising given that in order to use private IT for a business purpose, one must first purchase it and bring it into the workplace.

In the specific context of mobile technology use for business purposes, ORP may take the form of activation of work email on a private device. If an employee purchases a mobile device, requests corporate email access on their private device, and has this access approved and provision by the IT department, they are engaging in the authorized use of private IT for business purposes. On the other hand, if an employee does not request access, and instead bypasses the IT department by setting up a connection to the enterprise email server on their own, they may be engaged in the unauthorized use of private IT for business purposes.

With respect to the triggers that link preconditions for boundary blurring to the various end states, task compensation, being in an emotional state of anxiety or stress and having a desire to alleviate this feeling, could lead to the use of private IT for private purposes (Schalow et al. 2013). When an employee is engaged on a work assignment, and feels that they need a break, they may choose to browse their personal social networks such as Facebook or Twitter. Doing so on a private mobile device during work hours may constitute an unauthorized use of private IT, depending on the organization's IT policy.

Task optimization, a desire to improve task performance, could also lead to authorized or unauthorized use of private IT for business purposes (Schalow et al. 2013). Employees who have been provisioned with business IT such as a mobile device or laptop may find that they are able to perform certain tasks better using their own IT devices (Harris et al. 2012). This could be a result of the constraints of the business IT, or the affordances of private IT. Affordances and constraints arise when a technology either supports or restricts an individual's agentic desire (Leonardi 2011). For example, employees who are creating a creative document like a brochure or presentation may find that they are better able to do so using the software and functionality provided by Apple MacBook laptop computers. If the organization has not made these available for employees, the employee may choose to complete the design-oriented task using their own device. In such instances, the employee is engaged in the use of private IT for business purposes. Again, depending on how the organization's information security policy treats such IT use, it may either be authorized or unauthorized.

As can be seen, steps have been taken towards developing a identifying the precursors and triggers of IT Consumerization within organizations. Our aim is to present a model of private IT use in organizations that can be used to theorize on the different paths towards IT Consumerization, and their impact to organizations and employees.

A Model of Private IT Use in Organizations

In this section, we build on prior literature and present our model of private IT use in organizations. The first step in developing our research model is to identify all of the activities and triggers that can lead to the various categories of private IT use in organizations. Activities differ from triggers in that activities are observable actions taken by an individual or organization where as triggers are the underlying causes or cognitive processes that catalyze those activities. In our proposed model (see Figure 2), employees can be in one of four private IT use states with respect to a specific task or technology: No private IT use (Px), the use of private IT for private purposes (Pp), the unauthorized use of private IT for business purposes (UAPb) or the authorized use of private IT for business purposes (APb). They may remain in one state indefinitely, or move to another state given an activity and its trigger.

Own resource provision (ORP), purchasing and brining one's own IT in to the workplace, is a necessary activity to move from Px to any of the other states. As noted in prior IT Consumerization research, task compensation will trigger a shift from Px to Pp where as task optimization can lead to either UAPb or APb. The presence or absence of effective rules set by the organization (ERSO) will determine whether

[3] We have chosen not to include use of private IT for teleworking in our model as we do not feel it is theoretically distinct from UAPb or APb

the employee ends up in UAPb or APb, as it is an indicator of Business-IT Alignment (BITA). Business-IT alignment is a snapshot of an organization's ability to fulfill business needs with IT capabilities (Györy et al. 2012). If the organization has set effective rules, such as a BYOD policy, governing the use of private IT within the enterprise and employees have a desire to use private devices for business purposes, then we can say that the organization is exhibiting strong Business-IT Alignment. In such instances, ORP will lead to the authorized use of private IT for business purposes. On the other hand, if the organization has not recognized the possibility that employees may wish to use their own IT within the workplace and developed an effective set of rules around this, it is exhibiting poor Business-IT Alignment and unauthorized uses of private IT for business purposes will arise (e.g. Shadow IT, Györy et al. 2012).

Discontinuation of the use of private IT, either entirely (returning to the Px state) or for business purposes (returning to the Pp state) can result from one of two causes. If the employee is currently in the Pp state, discontinuation will result from organizational security, education, training and awareness (SETA) programs combined with IT monitoring software. General deterrence theory (Gibbs 1975) argues that increasing the perceived certainty or severity of punishment is a means of preventing crime in the general population. In the context of IT misuse or abuse in organizations, SETA programs such as formal communications and in-class or computer-based training can increase the perceived severity of punishment by making employees more aware of the consequences for IT misuse/abuse. On the other hand, the use of IT monitoring software, such as software to monitor network traffic within the organization, can increase the perceived certainty of punishment by making employees aware that their actions are being monitored regularly. The combination of SETA and IT monitoring has been shown to reduce IT misuse intention in studies of computer users within organizations (D'Arcy et al. 2009), therefore we expect the presence of both to trigger discontinuation of the use of private IT for private purposes, particularly where this behaviour is in violation of an organization's ISP.

If an employee is in the UAPb or APb state, discontinuation of the use of private IT for business and a return to either the Px of Pp state will be triggered by disconfirmation. According to expectation-confirmation theory (Oliver 1980), customers form their repurchase intention for a product or service based on their initial expectations and perceived performance of the product/service. Where perceived performance meets or exceeds their expectations, they will experience a confirmation and have greater satisfaction and repurchase intentions. On the other hand, if perceived performance falls below initial expectations, the individual will experience a disconfirmation and choose not to repurchase the product/service. In the context of IT use, continuance intention has been shown to result from whether perceived usefulness meets or falls below initial expectations (Bhattacherjee 2001). Therefore, if employees find that their use private IT of for business purposes (authorized or unauthorized) does not meet their initial expectations, they will discontinue use and return to the Px or Pp state.

If an employee has provisioned their own IT and is either using it for private purposes (Pp) or authorized business purposes (APb), they may begin to experiment with different uses and move into the UAPb state. For example, if an employee is using their own personal laptop for personal email communications (Pp) and wants to see if they can use it for work email as well, they may try to set up a connection to the corporate email server on their own (UAPb). Similarly, if an organization allows its employees to use a personal tablet device to store non-client related documentation (APb) and an employee wishes to use it for an upcoming client presentation, they may load the presentation on their device and take it with them to the client site (UAPb). Given that such an actions would be contrary to an organization's ISP, they represent forms of delinquency. According to neutralization theory (Sykes and Matza 1957) delinquency arises from defenses to crimes in the form of justifications for deviance. The five forms of justification that can occur are denial of responsibility, denial of harm, denial of the victim, condemnation of the victims or the appeal to higher loyalties. In the context of IT use within organizations, these neutralization techniques have been shown to increase an employee's intention to violate IT security policies (Siponen and Vance 2010). Therefore, we expect that neutralization techniques will trigger the experimentation that moves an employee from Pp or APb to UAPb.

Finally, if the employee is in the Pp state or UAPb state, they will move to the authorized use of private IT for business purposes when effective rules are set by the organization. The trigger for such a move, however, will differ based on the originating state. If the employee is currently using private IT for private purposes, and the organization introduces effective rules for the use of private IT for business purposes, task optimization will trigger their shift into the APb state. On the other hand, if the employee is engaged in Shadow IT (UAPb) and the organization introduces rules governing the use of private IT for business purposes, the presence of SETA and monitoring will trigger employees to restrict themselves to authorized uses of private IT only (APb).

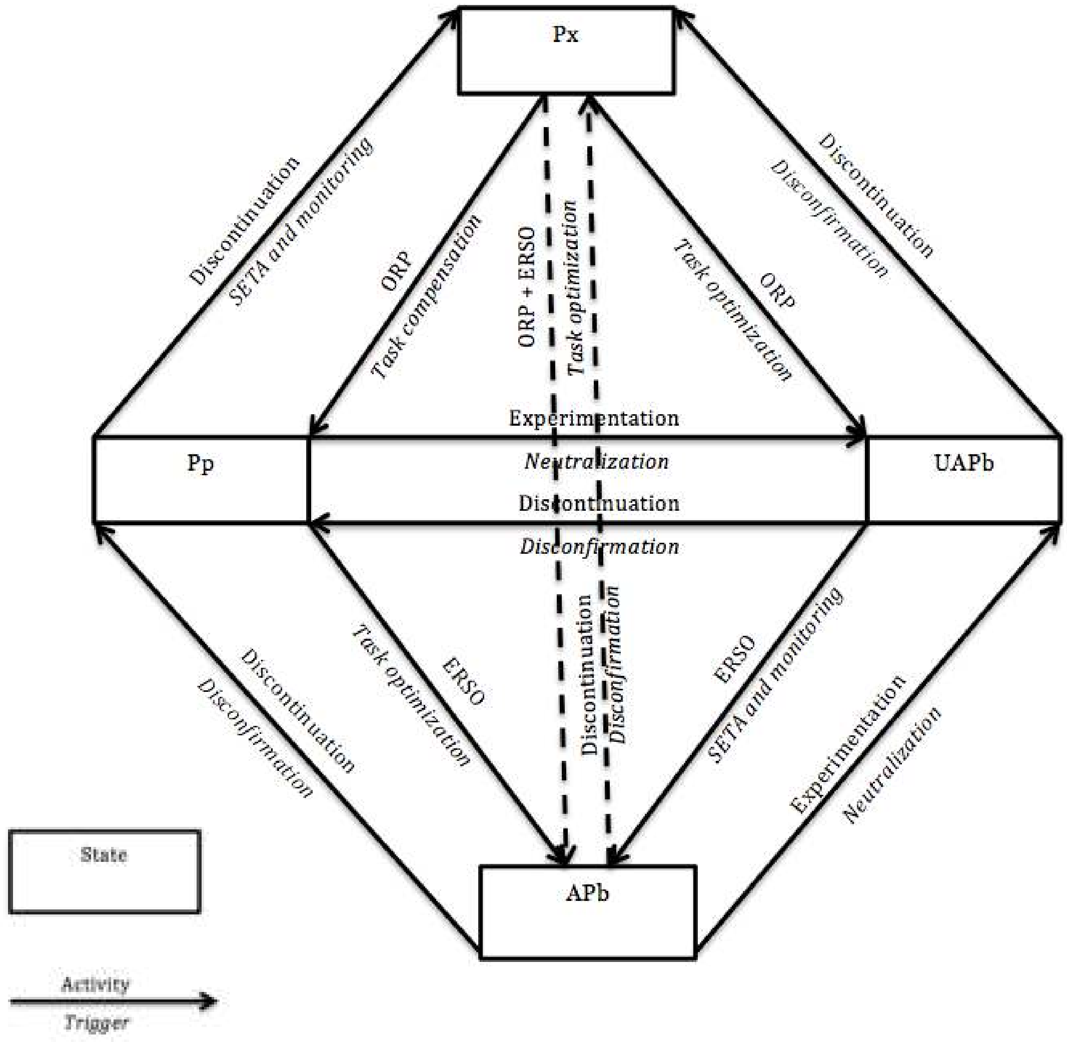

Figure 2 – Proposed Research Model

Paths Toward IT Consumerization

In this section we theorize around the different IT Consumerization paths that can unfold in an organization and highlight a set of research questions for each path. With conclude with a discussion of our next steps and expected contributions.

Based on our proposed research model, we can identify two distinct paths towards IT Consumerization: Employee-Driven Consumerization and Organization-Driven Consumerization. In the Employee-Driven Consumerization path, employees are motivated to provision their own IT and use it for business purposes because they believe it will lead to improved performance (Px->UAPb), or because they have a desire to experiment with different usage scenarios (Pp->UAPb). This leads to instances of Shadow IT where the business use of private IT is taking place outside of the monitoring and governance of the organization. When IT incidents occur, or the organization becomes aware of these unauthorized activities, they may respond by introducing a set of rules defining authorized use of private IT for business purposes. If these rules are combined with adequate education, training, awareness and monitoring, employees will be incented to follow them (UAPb->APb). Otherwise, employees will continue with their unauthorized use of private IT, thus creating a major risk to the organization.

In the Organization-Driven Consumerization path, the organization pre-empts unauthorized uses of private IT by recognizing the desire of their employees to use private IT for business purposes and creating a set of rules to govern this activity (Px->APb, Pp->APb). In so doing, the organization is able to minimize the threat of IT incidents that can occur when instances of Shadow IT arise within the organization. The motivation for employees to use private IT for business purposes is also different in this path. Where the Employee-Driven Consumerization path required SETA and monitoring to enforce the new set of rules governing IT use, Organization-Driven Consumerization instead relies on the employee's desire for task optimization to trigger the shift in use states. Therefore, compliance with the new organizational IT policy and overall impression of the organization may differ depending on which IT Consumerization path unfolds.

Within each IT Consumerization path, there are a number of unique research questions that can be addressed. For example, in Employee-Driven Consumerization, studies that identify the characteristics of employees who experiment with business uses of private IT would be a valuable contribution. Understanding the underlying personality and cognitive traits that make an individual more or less likely to stray from an organization's ISP advance the literature on attitude towards blurring boundaries (Schalow et al. 2013) and ISP compliance (Bulgurcu et al. 2010). Constructs that might be incorporated in future studies include Personal Innovativeness with IT (Agarwal and Prasad 1998) or the Five Factor Model of personality (Devaraj et al. 2008). Findings from these future studies could also help organizations better direct their efforts at establishing effective rules, and can also help foster a greater understanding of how the IT Consumerization trend took hold.

In the Organization-Driven Consumerization path, a key factor in determining the outcomes that are achieved is the timing of the organizational intervention (i.e. establishing effective rules). The combination of a real-time longitudinal study with multiple retrospective case studies may be an innovative approach to exploring this phenomenon (see Leonard-Barton 1990). This would allow the researcher to establish that timing of the organizational intervention can impact if and when unauthorized uses of private IT arise, and then focus on a single organization to understand how this process unfolds. A mixed methods approach (Venkatesh et al. 2013) could also be employed to demonstrate that the decision criteria leading to authorized uses of private IT (desire for task optimization vs. compliance with the organization's ISP) differs based on the timing of organizational intervention. The first part of such a study would employ qualitative research methods such as interviews and observation to identify the various factors that individuals consider when using private IT for a business purpose, and then follow up with a quantitative survey methodology to determine if the strength of these factors differ in organizations where ERSO either preceded or followed IT incidents and instances of Shadow IT.

Next Steps and Expected Contributions

This research-in-progress manuscript will be presented at a roundtable session taking place at the DIGIT 2014 Pre-ICIS workshop in Auckland, New Zealand. Feedback received will be incorporated into a final version which we plan to submit to a peer-reviewed IS journal. If future research empirically tests and validates the paths hypothesized in this model, it has the potential to represent a significant contribution to both research and practice. From a theoretical perspective, we will be extending prior work on the precursors and triggers of IT Consumerization by including constructs from general deterrence theory, expectation-confirmation theory and neutralization theory, and presenting a model of the various private IT use outcomes that can occur within organizations. From a practical perspective, our model can serve as useful roadmap for IT leaders within organizations. By identifying their current state on a particular IT Consumerization path, IT decision-makers can determine how various organizational and employee activities will lead to different uses of private IT within the workplace. The organization may then choose to pre-empt Shadow IT by recognizing a desire for task optimization on the part of their employees and introducing a BYOD policy instead. In so doing, they will be able to monitor and govern the use of private IT for business purposes rather than waiting for IT incidents to occur.

References

Agarwal, R., and Prasad, J. 1998. "A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology," (9:2), pp. 204–216.

Bhattacherjee, A. 2001. "Understanding information systems continuance: an expectation-confirmation model," *MIS quarterly* (25:3), pp. 351–370.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS quarterly* (34:3), pp. 523–548.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98 (doi: 10.1287/isre.1070.0160).

DeSanctis, G., and Poole, M. 1994. "Capturing the complexity in advanced technology use: Adaptive structuration theory," *Organization science* (5:2), pp. 121–147.

Devaraj, S., Easley, R. F., and Crant, J. M. 2008. "Research Note —How Does Personality Matter? Relating the Five-Factor Model to Technology Acceptance and Use," *Information Systems Research* (19:1), pp. 93–105 (doi: 10.1287/isre.1070.0153).

Gibbs, J. P. 1975. *Crime, Punishment and deterrence*, New York: Elsevier.

Györy, A., Cleven, A., Uebernickel, F., and Brenner, W. 2012. "Exploring the shadows: IT governance approaches to user-driven innovation," in *ECIS 2012 Proceedings. Paper 222*, http://aisel.aisnet.org/ecis2012/222/.

Harris, J., Ives, B., and Junglas, I. 2012. "IT Consumerization: When Gadgets Turn Into Enterprise IT Tools," *MIS Quarterly Executive* (11:3), pp. 99–112.

Leonard-Barton, D. 1990. "A dual methodology for case studies: synergistic use of a longitudinal single site with replicated multiple sites," *Organization science* (1:3), pp. 248–266.

Leonardi, P. 2011. "When Flexible Routines Meet Flexible Technologies: Affordance, Constraint, and the Imbrication of Human and Material Agencies," *MIS quarterly* (35:1), pp. 147–167.

Niehaves, B., Köffer, S., and Ortbach, K. 2012. "IT Consumerization–A Theory and Practice Review," in *Proceedings of the Eighteenth Americas Conference on Information Systems*, Seattle, Washington, USA.

Oliver, R. 1980. "A cognitive model of the antecedents and consequences of satisfaction decisions," *Journal of marketing research* (17), pp. 460–469.

Ortbach, K., Bode, M., and Niehaves, B. 2013. "What Influences Technological Individualization?–An Analysis of Antecedents to IT Consumerization Behavior," in *Proceedings of the Nineteenth Americas Conference on Information Systems*, Chicago, Illinois, USA, pp. 1–9.

Schalow, P., Winkler, T., Repschlaeger, J., and Zarnekow, R. 2013. "The Blurring Boundaries Of Work-Related And Personal Media Use: A Grounded Theory Study On The Employee's Perspective," in *ECIS 2013 Completed Research. Paper 212*, http://aisel.aisnet.org/ecis2013_cr/212 .

Siponen, M., and Vance, A. 2010. "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS quarterly* (34:3), pp. 487–502.

Sykes, G. M., and Matza, D. 1957. "Techniques of Neutralization: A Theory of Delinquency," *American Sociological Review* (22:6), pp. 664–670 (doi: 10.2307/2089195).

Venkatesh, V., Brown, S., and Bala, H. 2013. "Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems," *Mis Quarterly* (37:1), pp. 21–54.