

Special Issue on “Dark Side of Information Technology Use”: an Introduction and a Framework for Research

Forthcoming in *Information Systems Journal*, 25,3

doi: 10.1111/isj.12070

Monideepa Tarafdar (m.tarafdar@lancaster.ac.uk)

Ashish Gupta (Gupta@utc.edu)

Ofir Turel (oturel@fullerton.edu)

Abstract

We introduce the Special Issue on “Dark Side of Information Technology Use”. We first provide a brief summary of the literature and suggest a framework as guidance for future research on dark side phenomenon. We then comment on and characterize the papers presented in this Special Issue using this framework.

We do not ride on the railroad; it rides upon us – Henry David Thoreau, 1854

1. Introduction

We see the “dark side” of IT use as a broad collection of ‘negative’ phenomena that are associated with the use of IT and that have the potential to infringe the wellbeing of individuals, organizations and societies. Early understanding of the negative consequences of IT use focused on IT mediated control of individuals in the workplace made possible by the automatic and electronic capture of information generated by tasks and activities (Zuboff 1988), workflow rigidity caused by computer-integrated manufacturing systems (Corbett et al. 1989), decreased interpersonal interaction and social support from use of electronic performance monitoring systems (Carayon 1993), psychological effects on individuals such as computer anxiety (Heinssen et al. 1987) and workplace stress, and technical vulnerabilities such as Y2K. Other negative consequences studied were among others, loss of employment due to computerization, thefts of intellectual property and identity, ergonomics-related injuries, and software-related accidents (Kling 1996).

While this early understanding helped sensitize IS and management researchers to the potentially negative impacts of IT use, current trends have dramatically increased the potential ambit, scope and intensity of dark side phenomena. First, increasing reach (Keen 1991) of IT enables use by people from a variety of demographic backgrounds and locations for work and non-work tasks, implying increased pervasiveness of IT-mediated activity. Second, increasing richness (Rayport and Sviokla 1995) makes for IT products and applications that can be flexibly customized to individual user requirements through software components injected into hardware. Third, increasingly user friendly, reliable and embedded IT are paving the way for its decentralized, un-guided, and continuous use.

One fall-out of these trends is that users experiment and improvise (Ciborra 1985) in how they use system features. Such experimentation can have unexpected, designer-unintended and potentially negative consequences for the user and the social unit where IT is being used. For example, the same software that is designed for testing network security and vulnerability by corporate IT or law enforcement departments, can also be used for illegal network hacking and break-ins. Further, it is not possible for system designers or users to anticipate and foresee all of these negative consequences (Markus and Mentzer 2014). Another fallout is that IT-mediated activities generate data that is easily stored, manipulated, analysed and accessed. Much of this data resides in the thin space between individuals' right to privacy and ownership and the collective's use of them for profit, surveillance and common-good activities; the possibilities for dark side phenomena abound.

Recent studies have therefore examined a number of emerging phenomena associated with the negative consequences that may be experienced by individuals, such as technostress, technology addiction, technology-induced interruptions, information overload, and deviant IT-use behaviours by employees in organizations. In this Special Issue, and as stated in its call-for-papers, we build on this stream to explore "complex social and individual situations where the very benefits that the use of IT brings contain the seeds of potentially transformative negative changes in ways of working, collaborating and living - changes that can lead to non-beneficial, if unintended consequences."

2. Current Research: Theorizing Dark Side Phenomenon

Theories that have traditionally informed studies on the negative impacts of IT have included economic approaches to study labor-capital substitution and sociological approaches to understand IT-enabled control. In more recent studies, given the large scope and variety of emerging and potential dark side phenomena, we find the opportunity to examine theories from a number of disciplines in explaining negative impacts associated with the use of IT.

As examples, in studies on technostress for instance, transaction and coping theories of stress from psychology (Lazarus and Folkman 1964) have been used to identify conditions pertaining to IT use that create chronic conditions of stress in the workplace and associated potential inhibiting mechanisms (Ragu-Nathan et al. 2008) as well as the negative outcomes (e.g. Ayyagari et al. 2010). Meanwhile, moral disengagement theory has been used to explain coping mechanisms (D'Arcy et al. 2014), and social cognitive theories have been used to identify mechanisms for countering the effects of technostress (Tarafdar et al. 2015b). The concept of the panopticon (Bentham 1787/1995)

has been used to characterize the dark side of IT-based surveillance and control (Zuboff 1989). Studies of technology addiction have been informed by theories of substance (Robinson and Berridge 2003) and behavioural (Turel et al 2011b) addiction, and by the Diagnostic and Statistical Manual criteria for problematic behaviors and addictions (American Psychiatric Association 2000). For studying IT induced interruptions and multitasking behaviors, distraction conflict theory (Baron, 1986) provides a theoretical perspective for understanding the distribution of attention between the primary task and the interruption. A workflow and process-oriented approach to analyzing IT-based interruptions enables identification of impacts on performance of critical tasks (Gupta et al. 2013a).

3. Looking Forward: Themes for characterizing the dark side and directions for future research

We note here that ‘dark side’ is an over-arching term that includes several phenomena, some of which have been studied, many which have not, and perhaps many more that have not yet been actuated. We suggest that it is useful at this stage, as guidance for future research, to identify salient themes according to which these phenomena can be classified. Looking forward, we develop a framework (Figure 1) that can be used as basis for future research on dark side phenomena. It describes four themes - context of their occurrence, negative outcomes, mitigation mechanisms and level of analysis. The first three themes characterize key aspects of dark side phenomena and the fourth suggests that these aspects can be investigated at different levels of analysis.



Figure 1: Framework for characterizing dark side phenomena

3.1. Context of Occurrence

‘Context’ refers to the specifics of a given situation in which IT is used or developed (Lee and Baskerville 2003). Given the increasing variety of IT users and usage situations, and given that those characteristics of IT that make it useful are also key enablers of dark side phenomena, dark side behaviours and outcomes depend on the context. Zimmerman et al (2007) describes five elements of context that are salient in this respect, viz.: individuality (e.g. individual characteristics, demographic groups), activity (e.g. task), location (e.g. spatial or physical setting), time (e.g. temporal characteristics), and relations (e.g. how different individuals are related).

To exemplify these elements, individuals, depending on factors such as age and polychronicity (the natural tendency to engage in multi-tasking) (Conte and Gintoft 2005), may have different propensities to suffer from dark side consequences of IT-based interruptions. Such findings convey the importance of tailored technology design and push technology designers away from the 'one technology fits all' paradigm. Second, in terms of tasks, as more organizational functions and units are expected to be involved in dark side phenomena (Tarafdar et al. 2015a), there is a need to understand the different activities where dark side phenomena can occur. Third, in terms of location, the effects of phenomena such as interruptions and IT addiction have been studied in work and non-work contexts (Chen and Karahanna 2014, Turel et al. 2011a). Increasingly however, use of IT takes place both continually, that is, not confined to a specific physical location, and seamlessly across life-activities, that is, not easily classified as 'work' or 'non-work'. This is possibly more so for digital natives (Vodanovich et al. 2010). Future research should thus also examine dark side phenomenon in such 'virtual' milieus. Fourth, it is possible that the effects of dark side phenomena are manifested differently over time. For example, while multitasking may lead to instant task accomplishment in the short term, it may cause productivity loss or poor health in the long term. Fifth, consideration of how individuals are related provides the opportunity for understanding group level phenomena. For example, social media-enabled and rapid rumor spreading in times of natural and human-precipitated disasters can thwart public safety and rescue efforts; social networks and relationships become particularly potent during such incidents.

3.2. Negative Outcomes

Dark side phenomena, by definition are associated with various negative outcomes. We see four aspects of negative outcomes: individual, organization, industry and society. Outcomes for individuals have included those that are adverse workplace job and task related (e.g. Gupta et al. 2013b, Selander and Henfridsson 2012), problematic/deviant IT use related (e.g. Turel et al. 2011b, D'Arcy et al. 2014), and work-life conflict related (Turel et al. 2011a, Chen and Karahanna 2014). Organizational outcomes studied have included reduced employee commitment, security breaches and employee turnover (Tarafdar et al 2015a). There is potential for research that examines the impact of the individual's dark side cognitions and behaviors on organizational outcomes such as efficiency, productivity, reputation and financial performance.

The mortgage and related financial services industry provides a good example for industry related outcomes. Standardization of IT applications used in the mortgage industry, while enabling process

efficiencies through automated under-writing systems, might also have been associated with a decline in under-writing standards and a focal point for co-evolving industry changes such as lender-concentration, increased sub-prime lending, and easy/quick trading of mortgage-backed financial securities (Markus and Mentzer 2014). These effects may have been major contributors to the 2008 global financial crisis. To give another example, high-speed trading systems have been known to cause "flash crashes": research (reported in Tracy and Patterson 2014) shows that a key reason for these crashes is the use of super-fast, automated trading algorithms that obtain asymmetrically early access to price and policy information published by trading firms through high speed IT networks. During one such crash that occurred in May 2010, the Dow Jones Index fell an unprecedented 1000 points in the space of a few minutes (Smith 2014), as USD 1 trillion was wiped off the value of markets; profits from such crashes often accrue to a miniscule percentage of those who participate in the stock markets. Studies of similar phenomena would be helpful in understanding industry-level dark side aspects.

Although past research has examined societal impacts such as lack of work life balance (Ahuja et al. 2007), the area of dark side outcomes at the societal level remains largely unexplored. There is strong interest in examining the societal impacts of IT (Majchrzak et al. 2014). Taken together with the dark side imperative, there is thus particular interest and scope for research in this area. In terms of societies and nations, future research could focus on potential outcomes in terms of information exclusion (e.g. Castells 1996), disruptive patterns of work/living, Internet crime and pornography, identity theft and related issues, cyber-attacks and loss of privacy.

3.3. Mitigation Mechanisms

Mitigation mechanisms are important because they can alleviate dark side phenomena and/or their negative outcomes (e.g. Nelson and Kletke 1990). Pre-emptive mechanisms could be interventions that make a particular dark side phenomenon less likely to occur. They could be measures such as identifying and reducing the number of IS design features likely to cause stress, overload or addiction for instance, a fruitful area for future research. Another potentially fruitful area is the pre-emptive design of organizational policies regarding use of common applications such as email and social networks. Other mitigating mechanisms might be directed at the individual to alleviate his or her dark side behaviors and attitudes after they are manifested. These could include workplace mechanisms directed towards employees such as education/counselling, awareness, institutional support, job/role re-design and altered reporting structures. They could also comprise educational and social support at the level of the family and other social units, for creating awareness of IT

addiction, cyberbullying, Internet pornography, privacy problems and intellectual property theft. While some mitigating mechanisms have been suggested (Tarafdar et al 2015a), research in this area is relatively sparse.

We also see legal, civic and political policies as powerful mitigation mechanisms. Similar to policies on health, we are now seeing the wide-scale deployment of policies shaping IT use activities such as checking email (Stuart 2014). National policies which are relevant for dark-side IT phenomena may include, for instance, restricting access to potentially harmful or dangerous websites (for instance, child pornography) (Quayle et al. 2002), ensuring cyber-security (Givens et al. 2013) and developing appropriate industry-specific regulations, such as in the financial sector.

3.4. Level of Analysis

It is important to study the level of analysis of dark side phenomena because IT use causes changes in the work and lives of individuals, organizations and other social collectives. Much of the recent research cited in this editorial introduction has focussed on the individual level of analysis in terms of the individual's experience and behaviour regarding dark side phenomena. Associated outcomes such as impaired task performance and negative job attitudes have also been examined at the individual level (e.g. Tarafdar et al. 2015b). However, these individual-level effects can also have repercussions in teams, families and organizations. For example IT addiction can increase conflicts between family members and the intention to switch jobs (Turel et al. 2011a) while misuse of IT or non-compliance with organizational security policies may have financial- or reputation-related organizational implications. Equally, individual level variables such as misuse can be affected by organizational level variables such as leadership, culture or IT use policies (D'Arcy et al. 2009), or national/societal level variables such as general work-culture and government policies (Xu et al. 2012). Thus, we call for attention to levels of analysis other than the individual, and to cross-level effects, i.e., when predictors at one level influence outcomes at a different level.

Further, a particular dark side phenomenon may exhibit a temporal progression from one level to another or within the same level. For instance prolonged misuse of IT by individuals, if unchecked, might eventually lead to loss of sensitive organizational data, or prolonged exposure to techno-stressors might lead to negative impacts on health. Accordingly, appropriate policies at national and organizational levels may lead, over time, to reducing the frequency of occurrence of dark side phenomena, as has been seen in the case of temporal impacts of government policies on smoking

and drinking (e.g. Ponicki et al. 2007). Thus longitudinal studies tracing particular phenomena over time and across levels represent another fruitful avenue for research.

Dark side phenomena can be studied using the qualitative and quantitative approaches typically employed in IS research. In addition, given that the negative consequences of IT use are largely unintended and unforeseen by designers, the use of future-oriented approaches such as scenario planning (Markus and Mentzer 2014) can provide foresight about possible system uses and thus sensitize IS designers to the proactive anticipation of potential dark side effects from their use. Further, design approaches that can offer persuasive support at the moment of use (Fogg 2002) or utilize concepts such as value-based design (Schwartz 1994) could be used to design IS for minimizing dark side effects. For instance, one may examine how interventions at the moment of use might lead to better interruption/overload handling, multi-tasking or overuse management. Experimental designs that capture IT use in meaningfully simulated environments have the potential to reveal dark side use behaviours.

4. Contribution of Papers

In response to our call for papers for the Special Issue on the Dark Side of IT in the Information Systems Journal, we received a large number of manuscripts, each of which went through the Journal's peer review process consisting of reviewers' comments and editorial feedback from the Associate Editors and Guest Editors of this Special Issue. The final set of papers went through two or three rounds of review and revisions. They are diverse in terms of author demographics and AIS region affiliations. We are deeply grateful to the Associate Editors and reviewers, who put in many hours of work in order to help the authors of the papers we present here, improve their works. This special issue would not be possible without their commitment, dedication and hard work. We thank the Journal's Editors for their support with this Special Issue.

In this first part of the Special Issue, we present a collection of four papers that report on studies on familiar and new dark side phenomena, conducted in different contexts and associated with different negative consequences. We characterize the papers using the framework developed in this editorial. We note here that most of these papers address the individual level of analysis and do not address mitigation mechanisms. This is representative of the total set of papers that were initially submitted; these 'missing' themes point to areas we see as being important to future research.

The paper "*Illuminating the Underground: The Reality of Unauthorised File Sharing*" by Beekhuyzen, J., von Hellens, L., and Nielse. S., explores a relatively unexamined type of online community, namely

one that focuses on the illegal sharing of music files. This is perhaps not a new dark-side phenomenon, but the IS literature is relatively silent about it. In this study the authors contribute by theoretically developing this context, explaining the nature and formation processes of such communities and systematically exploring the reasons for engaging in such illicit behaviors. The overarching theoretical perspective is Actor Network Theory. The study's findings, based on qualitative data, describe negative outcomes at multiple levels and indicate that people engage in such illicit behaviors because the resources they seek are scarce in traditional markets. The **context** for the study is an online community focused on the free and unauthorised sharing of music files. **Negative outcomes** include, for individuals, possible legal actions which can result in fines and jail time, for online communities, legal action and dismantlement, and for the music industry, financial damages. The phenomenon is analyzed at the **level of individual** participants, the online community and the music industry. Given the growth of illegal file sharing and associated problems, this paper presents a topical issue.

The paper, *"Leveraging fairness and reactance theories to deter reactive computer abuse: An empirical study of the influence of counterfactual reasoning and organizational trust"*, by Lowry, P., Posey, C., Bennett, R., and Roberts, T., uses fairness and reactance theories to explain security-related reactions to unfair events that result in reactive computer abuse. This study explains how factors such as explanation adequacy, trust, age, organizational security awareness, training and education, and computer use at work, could influence the formation of a dark side phenomenon such as computer abuse. It emphasizes how certain training and security programs could result in negative outcomes for the organization if employees are ignored. The **context** for the study is employees' use of IT in organizations from the banking, financial and insurance sectors in the US. The data is quantitative, from a survey administered to working professionals. **Negative outcomes** relate to abuse of computers detrimental to the organization analysed at the **level of individual** behaviour. This study could lead to initial work on integrating other theories such as Justice Theory to understand employees' reactive computer abuse.

The paper, *"The Effects of Technostress and Switching-stress on Discontinued Use of Social Networking Services: A Study of Facebook Use"*, by Maier, C., Laumer, S., Weinert, C., and Wetzels, T., examines technostress in the context of switching from one social network application to another. It extends the literature by conceptually developing the association between technostress and IT use discontinuance, and by developing the concept of switching stress creators, that is, the stress caused by switching from one application to another. It also focuses on system use termination, which few

studies have addressed so far and thus also extends the literature on adoption and usage phases of the IS life cycle. The **context** for the study is **individuals' use** of a social networking application (Facebook) in a non-work context. The data is longitudinal, collected through surveys, interviews, diaries and experiments at different points in time. **Negative outcomes** include exhaustion from social-network stress and switching stress experienced by the user and discontinued use of the application for the commercial application provider.

The paper, "*The Many Faces of IT Interruptions: A Taxonomy and Preliminary Investigation of Their Performance Effects studies*", by Shamel and Pinsonneault examines the effects of IT interruptions on productivity and develops a taxonomy of interruptions using data from qualitative log diaries of 14 participants and 21 qualitative interviews. The process of analysis leads the authors to define new categories of interruptions based on message content. The **context** for the study is individuals working on real, interdependent tasks within a larger project in an interruptive organizational work environment. **Negative outcomes** include interruptions and reduced task performance for individuals. The **level of analysis** is the individual's handling of interruptions. The study extends the IS literature on interruptions by suggesting that hybrid interruptions are neither completely relevant nor irrelevant to the task at hand. It adds to existing understanding of different interruption types and how they impact performance.

5. Conclusion

Research on the dark side of IT use can form an important bulwark of study in the IS field by reinforcing conceptual and critical richness in our research, and by providing a backdrop for mindful and thoughtful use of IT in its implications for impact and practice. Are we making a better world with ICT's? (Walsham, 2012); the theme of the 2014 International Conference on Information Systems was "Building a Better World through Information Systems". *The railroad need not ride on us*. We hope that this special issue will advance research on how various aspects of the dark side of IT use can be identified and countered.

6. References:

American Psychiatric Association. 2000. *Diagnostic and Statistical Manual of Mental Disorders-Text Revision*, 4th Edition. American Psychiatric Association: Washington, DC, USA:

Ayyagari, R., Grover, V. and Purvis, R. 2011 Technostress: Technological Antecedents and Implications, *MIS Quarterly* (35:4), 831-858.

Baron, R.S. 1986 Distraction–conflict theory: progress and problems, in: L. Berkowitz (Ed.), *Advances in Experimental Social Psychology*, Academic Press, New York.

Bentham, J. 1787/1995. *The Panopticon Writings*. Verso, London.

Carayon, P. 1993. Effect of electronic performance monitoring on job design and worker stress: review of the literature and conceptual model. *Human Factors* 35(3) 385-395.

Castells, M. 1996 *The Information Age: Economy, Society and Culture, The Rise of the Networked Society*, Blackwell, Oxford.

Chen, A., and Karahanna, E. 2014. Boundaryless Technology: Understanding the Effects of Technology-Mediated Interruptions across the Boundaries between Work and Personal Life, *AIS Transactions on Human-Computer Interaction*, (6:2) 16-36.

Ciborra, C. 2002 *The Labyrinths of Information, Challenging the Wisdom of Systems*, Oxford University Press.

Conte, J.M., and Gintoft, J.N. 2005. Polychronicity, big five personality dimensions, and sales performance, *Human Performance* (18:4), pp. 427–444.

Corbett, J.M. 1987. A psychological study of advanced manufacturing technology: The concept of coupling. *Behavior and Information Technology* 6(4) 441–453

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.

D'Arcy, J., Herath, T. and Shoss, M. (2014) Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective, *Journal of Management Information Systems* 31, 2, 291-325

Fogg, B.J. 2002 *Persuasive Technology: Using Computers to Change What We Think and Do*, Morgan Kaufmann, San Francisco, California.

Givens, A. D., and Busch, N. E. 2013. Integrating Federal Approaches to Post-Cyber Incident Mitigation, *Journal of Homeland Security and Emergency Management* (10:1). 1-19.

Gupta, A., Sharda, R., Dong, Y., Sharda, R (Jr), Asamoah, D., Pickering, B. (2013a), Improving Rounding in Critical Care Environments through Management of Interruptions, *Decision Support Systems*, (55:1), 516-527.

Gupta, A., Li, H., Sharda, R. (2013b) Should I send this Message? Understanding the Impact of Interruptions, Social Hierarchy and Perceived Task Complexity on User Performance and Perceived Workload, *Decision Support Systems*, (55:1), pp. 135-145

Heinssen, R.K., Glass, C.R. and Knight, L.A. 1987. Assessing computer anxiety: Development and validation of the computer anxiety rating scale. *Computers in Human Behavior* 3, 49-59.

Keen, P. 1991 *Shaping the Future*, Harvard Business School Press, Cambridge: MA

- Kling, R. (1996). *Computerization and controversy: value conflicts and social choices* (2nd ed.), San Francisco: Morgan Kaufman
- Lazarus, R.S., and Folkman, S. 1984. *Stress, appraisal, and coping*. Springer, New York.
- Majchrzak, A., Markus, M. L., and Wareham, J. (2013) *Call for Papers, MISQ Quarterly Special Issue on ICT and Societal Challenges*,
<http://www.misq.org/skin/frontend/default/misq/pdf/CurrentCalls/ICTChallenges.pdf>
- Markus, M, and Mentzer, K., (2014) Foresight for a Responsible Future with ICT, *Information Systems Frontiers* 16, 353-368.
- Nelson, D. L. and Kletke, M.G. 1990. Individual adjustment during technological innovation: a research framework. *Behavior and Information Technology* 9(4) 257-271.
- Quayle, E., and Taylor, M. 2002. "Child pornography and the internet: perpetuating a cycle of abuse," *Deviant Behavior* (23:4) 331-361.
- Ragu-Nathan, T.S., Tarafdar, M., Tu, Q. and and Ragu-Nathan, B.S. (2008) "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation," *Information Systems Research* (19:4), pp. 417-433
- Rayport, J.F., and Sviokla, J.J. 1995. Exploiting the virtual value chain. *Harvard Business Review* 73, 6, 75-84.
- Robinson, T. E., and Berridge, K. C. 2003. Addiction, *Annual Review of Psychology* (54) 25-53.
- Schwartz, S. H. (1994). Are there universal aspects in the structure and contents of human values? *Journal of Social Issues*, 50(4), 19–45.
- Selander, L. and Henfridsson, O. (2012), Cynicism as user resistance in IT implementation. *Information Systems Journal*, (22:3): 289–312.
- Smith, A. (2014), Fast money: the battle against the high frequency traders, *The Guardian*, June 07.
<http://www.theguardian.com/business/2014/jun/07/inside-murky-world-high-frequency-trading>
- Stuart, K. (2014) "German Minister Calls for Anti-Stress Law Ban on Emails out of Office Hours," August 29, <http://www.theguardian.com/technology/2014/aug/29/germany-anti-stress-law-ban-on-emails-out-of-office-hours>
- Tarafdar, M., D'Arcy, J., Turel, O., and Gupta, A. 2015a. The Dark Side of Information Technology, *MIT Sloan Management Review* (56:2), 600-623
- Tarafdar, M, Pullins, E and Ragu-Nathan, T.S., 2015b Technostress: Negative Effect on Performance and Possible Mitigations, *Information Systems Journal*, (25:2), 103-132.
- Tracy, R. and Patterson, S. (2014) Fast Traders Are Getting Data From SEC Seconds Early, *Wall Street Journal* October 29. <http://www.wsj.com/articles/fast-traders-are-getting-data-from-sec-seconds-early-1414539997?autologin=y>

Turel, O., Serenko, A., and Bontis, N. 2011a. Family and work-related consequences of addiction to organizational pervasive technologies, *Information & Management* (48:2-3) 88-95.

Turel, O., Serenko, A., and Giles, P. 2011b. Integrating Technology Addiction and Use: An Empirical Investigation of Online Auction Users, *MIS Quarterly* (35:4) 1043-1061.

Vodanovich, S., Sundaram, D. and Myers, M.D. (2010). Research Commentary – Digital Natives and Ubiquitous Information Systems, *Information Systems Research* 21(4): 711-723.

Walsham, G. (2012). Are we making a better world with ICTs? Reflections on a future agenda for the IS field. *Journal of Information Technology*, 27(2), 87–93.

Xu, Z. C., Turel, O., and Yuan, Y. F. 2012. Online game addiction among adolescents: motivation and prevention factors, *European Journal of Information Systems* (21:3) 321-340.

Zimmermann, A., Lorenz, A., Oppermann, R. (2007). An Operational Definition of Context, In B. Kokinov et al. (Eds.): *Modeling and Using Context, Lecture Notes in Computer Science* Volume 4635, 558-571, Springer-Verlag.

Zuboff, S. 1988. *In the Age of the Smart Machine: the Future of Work and Power*, Basic Books, New York.