Panel Report: The Dark Side of the Digitization of the Individual

Ofir Turel
College of Business and Economics, California State University, Fullerton, USA

Christian Matt
Institute of Information Systems, University of Bern, Bern, Switzerland

Manuel Trenz
Faculty of Business and Economics, University of Augsburg, Augsburg, Germany

Christy M.K. Cheung
Department of Finance and Decision Sciences, Hong Kong Baptist University, Hong Kong, People's Republic of China

John D'Arcy*
Department of Accounting & Management Information Systems, Lerner College of Business & Economics, University of Delaware, Newark, Delaware, USA

Hamed Qahri-Saremi*
College of Computing and Digital Media, DePaul University, Chicago, Illinois, USA,

Monideepa Tarafdar*
Management Science Department, Lancaster University (Management School), Lancaster, UK

Citation:

Ofir Turel, Christian Matt, Manuel Trenz, Christy M.K. Cheung, John D'Arcy, Hamed Qahri-Saremi*, Monideepa Tarafdar*, (2019) "Panel report: the dark side of the digitization of the individual", Internet Research, Vol. 29 Issue: 2, pp. 274-288, https://doi.org/10.1108/INTR-04-2019-541.*

* In Alphabetical order.

Abstract:

Digital technologies have diffused into many personal life domains. This has created many new phenomena that require systematic theorizing, testing and understanding. Such phenomena have been studied under the Digitization of the Individual umbrella and have been discussed in the Digitization of the Individual (DOTI) pre-ICIS workshop for the last three years. While prior years have focused on a variety of issues, this year we decided to put special emphasis on negative effects of the digitization of the individual, i.e., "the dark sides" of the digitization of the individual. This manuscript reports on a panel of three experts (in alphabetical order: John D'Arcy, Hamed Qahri-Saremi, and Monideepa Tarafdar) who presented their past research in this domain, as well as their outlook for future research and methodologies in research on the digitization of the individual. We introduce the topic, chronicle the responses of the panelists to the questions we posed, and summarize and discuss their response, such that readers can develop a good idea regarding next steps in research on dark sides of the digitization of the individual.

1. Introduction

Over the last two decades, digitally-supported technologies such as social media, video games, fitness trackers, autonomous cars, voice-activated personal assistants, smart watches, and robots have permeated personal life domains. This has created an array of cross-influences between personal, work and technology use domains (Piszczek et al., 2016; Yin et al., 2018), and blurred the boundaries between these domains (Chen and Karahanna, 2018; Ollier-Malaterre et al., 2013; Sarker et al., 2018). It has consequently led to the emergence of a range of new phenomena in the personal life domain, some of which can be positive for some users, for example the quantified-self (Barcena et al., 2014; Lupton, 2016), and others that are largely negative, for example, cyber-bullying (Chan et al., forthcoming), cyber-loafing with personal technologies at work (Khansa et al., 2017), and using social media while driving (Turel and Bechara, 2016). Realizing that such phenomena merit research attention, this is the third year in which we have organized a pre-ICIS workshop on the Digitization of the Individual (DOTI). This term encapsulates the penetration of digital technologies into individual users' lives. Under these circumstance, individuals typically have a major say in their own technology selection and usage decisions, and these choices are often at their own expense (Matt et al., forthcoming). Thus, the theories, management of and phenomena related to such technologies may differ from these employed in traditional work settings.

One area of the Digitization of the Individual that has not received much attention in a systematic fashion, is the dark sides of the Digitization of the Individual. Dark sides of technology use refer to negative, typically unplanned consequences of the use of technologies (D'Arcy et al., 2014a; Tarafdar et al., 2015b). Such issues permeate in adult workers (Tarafdar et al., 2013; Tarafdar et al., 2015a; Turel and Serenko, 2010; Turel, 2017), young-adult students (Turel and Bechara,

2017; Turel and Qahri-Saremi, 2016; Turel and Qahri-Saremi, 2018) and children alike (McHugh et al., 2018; Turel and Bechara, forthcoming; Turel et al., 2016; Turel et al., 2017). They can include a variety of issues pertaining to security and privacy, addiction, technostress, distraction, sleep hygiene, physical health, mental health and wellbeing, all of which may affect the use of digital technologies in the personal life domain and may be influenced by the Digitization of the Individual. Such effects can take place at all levels of analysis, ranging from the individual, to organizational to the national levels, as was pointed out in a Special Issue of Information Systems Journal on this topic in 2015 (Tarafdar et al., 2015b).

Notwithstanding the abovementioned special issue, there is a general paucity of systematic overview of such issues. We thus decided to organize a panel with three experts in different areas of the dark side of technology use. This manuscript aggregates their viewpoints, as expressed at the workshop. In this workshop, they discussed the current state of their own research related to dark side of use issues and the Digitization of the Individual, explained their motivation to focus on such issues, and elaborated on potential areas for future research as well as on potential methodologies to be used in Digitization of the Individual research. The three panelists in alphabetical order included: John D'Arcy, Associate Professor and the Robert and Kathy Deutsch Faculty Fellow in the Department of Accounting & Management Information Systems, Lerner College of Business & Economics, at the University of Delaware; Hamed Qahri-Saremi, Assistant Professor of Information Systems at the College of Computing and Digital Media, DePaul University in Chicago, Illinois; and, Monideepa Tarafdar, Professor of Information Systems, Lever Hulme Research Fellow, and Co-Director of the Center for Technological Futures at Lancaster University (Management School), U.K. The following sections outline the responses of these scholars to three questions that were discussed in the workshop.

2. What "dark sides" of DOTI do you study; and what motivated you to examine such issues?

D'Arcy: At a high level, my research focuses on the behavioral aspects of information systems (IS) security, which can be described as "the complexes of human action that influence the availability, confidentiality, and integrity of information systems" (Stanton et al., 2005). More specifically, I focus on the individual and organizational factors that contribute to employees' security-related behavior in the workplace. Such behaviors include those that are both positive and negative from an IS security perspective. Negative security-related behaviors include IS misuse, which is the "intentional misuse of computer systems by users who are authorized to access those systems and networks" (Schultz, 2002, p.526). IS misuse encompasses a broad spectrum of negative or improper computing acts, ranging from behaviors that are unethical and/or inappropriate (e.g., inappropriate use of e-mail and Internet privileges) to those that are illegal (e.g., stealing company information). At a more granular level, I study employee non-compliance with information security policies (ISPs). ISPs specify the proper uses of

organizational information and technology resources and include formalized sets of guidelines, procedures, and technical controls to which employees must adhere (Lowry and Moody, 2015). Research indicates that most organizations have ISPs in place, although ISPs can vary substantially in terms of scope and their enforcement (Goel and Chengalur-Smith, 2010). Common examples of ISP non-compliance include downloading and installing unlicensed (pirated) software, sharing passwords with co-workers, and using unapproved file sharing services, such as Dropbox. When such actions are prohibited by the organization, then they constitute ISP non-compliance. On the flip side, ISP *compliance* is a positive security-related behavior that I study. ISP compliance is distinct from ISP non-compliance in that compliance has some unique individual and situational antecedents (Cram et al., forthcoming). That is, ISP compliance and non-compliance are not simply two sides of the same coin. And, unlike ISP non-compliance, ISP compliance is beneficial from an IS security perspective because it helps reduce the risk of data breaches and other negative security events.

My motivation for studying the behavioral aspects of IS security dates back about 15 years. During this period of my PhD studies, I became interested in the emerging area of IS security. I found several industry reports which indicated that a large percentage of IS security incidents could be traced back to the behavior of employees (e.g., an employee failing to virus scan a floppy disk or an employee stealing company data and selling it to a competitor) (Ernst and Young, 2003; InformationWeek, 2005; Power, 2003). This finding was counter to the dominate view of IS security at time as being a purely technical topic. Indeed, during this period, most security experts were advocating investments in technical controls that detect and prevent externally initiated attacks as a means of achieving effective IS security strategy.

Today, most security experts recognize that consideration of both technical and human factors is essential for effective IS security. And, consistent with some of the earlier evidence that I noted above, recent statistics indicate that employees continue to be a "weak link" in organizational IS security efforts (Ponemon Institute, 2016; PwC, 2016). To this point, a content analysis of the descriptions of 2,633 publicly reported data breaches that occurred during 2005-2011 showed that a large percentage could be traced back to employee failure to follow proper security guidelines (Ayyagari, 2012). Within this analysis were breaches where employees failed to follow password policies, thus allowing an external hacker to access company data on a weakly-protected system. In other breaches, employees engaged in hacking activities themselves and stole company data either for resale or for personal criminal use. In still other breaches, employees engaged in more benign activities, such as leaving a file on a desk or failing to logoff a computer, which facilitated a breach that was perpetrated by a co-worker.

As I elaborate in my responses below, behavioral IS security issues are likely to remain an important topic for the foreseeable future, particularly in light of growing pressure on organizations to implement expanding security requirements and provide employees with ongoing security education and training. Such efforts trickle down to employees' day-to-day job duties, and in some instances, have been shown to induce negative security-related behavior (D'Arcy et al., 2014b; D'Arcy and Lowry, 2019; Posey et al., 2013).

Qahri-Saremi: (a) my research on the "dark sides" of digitization of the individual is focused on understanding problematic and addictive patterns of use of digital technology. I investigate the etiology of these, often unproductive, patterns of use of technology and how users respond to them. From the etiological perspective, I investigate the roles of cognitive systems (Turel and Qahri-Saremi, 2016; Turel and Qahri-Saremi, 2018) and user characteristics (e.g., Qahri-Saremi and Turel, 2016; Vaghefi and Qahri-Saremi, 2018) in developing problematic and addictive patterns of use of technology. Furthermore, the symptoms and negative consequences of problematic and addictive uses of technology can instigate cognitive, emotional, and behavioral responses from users. In my research, I strive to identify such user responses to the problematic and addictive patterns of use of technology and the factors that influence their formation and effects (e.g., Vaghefi and Qahri-Saremi, 2017).

(b) with the advancement and proliferation of digital technology, especially hedonic technology such as social media and video games, problematic and addictive patterns of use are increasingly prevalent and thus the magnitude of their consequences are higher than ever before. For example, at the individual level, technology addiction can reduce users' psychological wellbeing and mental health (Turel et al., 2018) and cause physical health problems such as sleep deprivation and debility (Salo et al., forthcoming; Turel et al., 2016; Turel et al., 2017). Similarly, at the organizational level, addictive use of technologies is associated with diminished organizational commitment (Turel and Serenko, 2010; Turel et al., 2011), risky information security behaviors, work exhaustion, reduced productivity, and job loss (Addas and Pinsonneault, 2018; Hadlington and Parsons, 2017; Mazmanian et al., 2013; Porter and Kakabadse, 2006; Venkatesh et al., forthcoming; Young, 2017; Young and Case, 2004). Furthermore, problematic uses of digital technology such as cyberloafing—defined as employees' non-work-related online activities while at work—is estimated to cost U.S. businesses as much as $85 billion annually in productivity loss (Hadlington and Parsons, 2017; Koay, 2018; Zakrzewski, 2016). This renders these patterns of use an important topic for research and motivates me to study them.

Tarafdar: The phenomena I study are associated with the technologies and applications that individuals use both with respect to work and outside work, such as email, general office technology and social media. A phenomenon I study is the stress that individuals experience, from using technologies in the workplace and outside, known as technostress (Ragu-Nathan et al., 2008; Tarafdar et al., 2007; Tarafdar et al., 2011; Tarafdar et al., 2013; Tarafdar et al., 2014; Tarafdar et al., 2015a; Tarafdar et al., 2015b; Tarafdar et al., 2015c). This includes different parts of the technostress process that include stressors, primary and secondary appraisals, coping and outcomes. I also study maladaptive uses of mobile technologies in the workplaces, especially by those who are mobile and span organizational boundaries in terms of executing customer facing processes, such as sales people(Bata et al., 2018; Ollier-Malaterre et al., 2013; Piszczek et al., 2016). While my primary motivation stems from the practical problems that these phenomena beget, the theoretical richness of these phenomena has also been a driving factor in my continued investigation of them.

One aspect that has intrigued me, theoretically, is that these phenomena are interdisciplinary. Theoretically speaking therefore, they allow us to investigate topics where traditionally IS research has not ventured into. Taking the example of technostress, while the phenomenon of

stress has been around for a long time, since the 1960's, the conceptualization of IS as a cause for stress is a much more recent one. The topic thus poses both an interesting challenge and a powerful opportunity for technostress researchers to contribute not only to the IS literature, but also to the stress literature. Tackling this issue, in a recent research paper (Tarafdar et al., 2019), we review the literature on technostress and develop a research framework to guide technostress research to make contributions that are not only disciplinary to IS but also "cross disciplinary" (Tarafdar and Davison, 2018), to the body of knowledge in psychological stress. It is worth noting that the IS literature on the dark side is now cited in papers from other disciplines (e.g., Karadağ et al., 2015; Nimrod, 2018).

3. It has now been a few years of a growing focus on the "dark sides" of the Digitization of the Individual; is this trend here to stay?

D'Arcy: I believe so and I will speak specifically in terms of my research on the behavioral aspects of IS security. Organizations are placing increasing reliance on ISPs and the associated security requirements, developed in part to guide employee compliance with external regulations such as the Sarbanes-Oxley (SOX) Act, The Health Insurance Portability and Accountability Act (HIPPA), The Payment Card Industry Data Security Standard (PCI DSS), and the European Union Data Protection Directive (EU DPD). The security requirements inherent in these and other government and industry standards related to IS security trickle down into the daily job activities of employees. For example, as described in my articles on security-related stress (D'Arcy and Teh, forthcoming; D'Arcy et al., 2014b; D'Arcy et al., 2018), there is evidence that employees are increasingly finding security requirements to be constraining, inconvenient, and difficult to understand. In terms of what may be producing such outcomes, employees are being subjected to more and more technical jargon in ISPs; they must also abide by ever changing rules regarding encryption of transmitted data and authentication procedures (e.g., when to use virtual private networks (VPNs)); and, at times, employees are forced to cease or slow down a specific job task to accommodate a centrally mandated security update on their computer. Situations such as these, which at first blush may seem innocuous, have been shown to induce stress in employees. Crucially, my research indicates that stress that emanates from security requirements can result in employee backlash toward their employers. This backlash can take the form of negative feelings toward the organization, such as frustration or a dissatisfaction (D'Arcy and Lowry, 2019; D'Arcy and Teh, forthcoming); or, more directly related to IS security outcomes, the backlash can include ISP non-compliance (D'Arcy et al., 2014b). In my estimation, this situation has the potential to become even more problematic in the future as organizations are forced to impose expanding security requirements on employees and subject them to ongoing security education, training, and awareness (SETA) efforts.

Related to this point, there is evidence that a new phenomenon—called "security fatigue" —is occurring in the workplace. Security fatigue refers to a socio-emotional state experienced by an individual who becomes tired and disillusioned with security-related initiatives (Cram et al., 2019). Research on security fatigue is at an early stage but it is thought that some employees may

experience security fatigue due to the abundance (and perhaps perceived overload) of security-related rules and communications that they experience. Notably, employees who experience security fatigue are distinct from those employees who consistently ignore or refuse to comply with ISPs. Rather, security fatigue is a gradual process experienced by employees who have been complying with security guidelines, but this adherence to guidelines becomes more burdensome and difficult over time. My preliminary research on security fatigue suggests that it too can lead to employees' non-compliance with ISP as well as a general minimization of effort toward IS security objectives (Cram et al., 2019).

My research on both security-related stress and security fatigue underscores the need for organizations to give continued attention to behavioral IS security issues, particularly in terms of how employees react to the bevy of security requirements that they encounter on a daily basis. For those employees who have high regard for their organizations, the increased stress and fatigue that comes from security requirements may be a non-factor, and these employees will continue to abide by ISPs and otherwise engage in positive security-related behaviors. But for those employees with weaker ties to the organization, and who perhaps feel slighted in some way (e.g., not getting a promotion), the stress and fatigue that comes from security requirements may draw them toward the "dark side" by means of engaging in negative security-related behavior. Future research is needed to explore these important issues in greater depth.

Qahri-Saremi: I argue that while the topics related to the dark sides of the digitization of the individual will evolve with the advancement of new and intelligent digital technologies, the "dark sides of digitalization" as a main research area is going to stay and expand. First, the digitization is not limited to only organizations or working professionals anymore. We now experience a proliferation of digitization in many aspects of the daily life (e.g., social media turning into a major source of information for citizens) that makes its effect more prevalent among a larger number of citizens. The proliferation of digitization will result in more users experiencing its unintended and negative consequences (i.e., "dark sides"). This trend is expected to augment the importance of research on the dark sides of digitization and identifying mitigating mechanisms for them.

Second, with the advancement of digital technology, we experience new types of digital systems, which can bring about new research topics within the domain of the dark sides of the digitization of the individual. An important case in point is the fast advancement of artificial intelligence (AI) and "algorithmic intelligence" that are dominating one domain after another in human lives. Algorithmic intelligence is increasingly shaping users' personality, judgements, emotions, and behaviors (Demetis and Lee, 2018; Markus, 2015; Markus, 2017; Yoo, 2015), so much that it has already impacted local traffic patterns (Yoo, 2015), stock prices (Demetis and Lee, 2018), criminal justice system (Walker, 2013), and even political elections (Persily, 2017), via its influences on human judgement and behaviors The fast rise of algorithmic intelligence and our fascination and dependence on it raises fundamental questions about *user control* (Demetis and Lee, 2018; Markus, 2017; Neff and Nagy, 2018; Yoo, 2015). In particular, intelligent digital technologies advance and become more autonomous, leading to more conflicts of autonomies and control with their human users (Markus, 2015; Markus, 2017; Yoo, 2015). Furthermore, the "systems of technologies" (Demetis and Lee, 2018) become more dominant,

leading to redefinition of and conflicts in user-system relationship. Therese are important and emerging areas of research within the dark sides of the digitization of the individual.

Tarafdar: I believe that as various technologies and applications further pervade processes of human activity both in the workplace and outside, we will see more negative phenomena and consequences associated with their use. The scope of dark side phenomena can only increase. The existing phenomena such as technostress, addiction, overload and work-life conflict (D'Arcy et al., 2014a; Tarafdar et al., 2015a; Turel et al., 2011) will be studied in the context of new technologies, while new phenomena will reveal themselves. Such expansion in conceptual scope can be vividly traced in the phenomenon of technostress. The early studies on technostress looked at the overall office technologies used by a broad section of employees (Ayyagari et al., 2011; Ragu-Nathan et al., 2008; Tarafdar et al., 2007). Later studies have expanded the scope, both in terms of the type of technologies and in terms of the kind of people. We have seen examples of the former where new aspects of technostress are being studied for different technologies such as social media and email (Maier et al., 2015; Salo et al., forthcoming; Stich et al., 2019). For the former, we have seen studies on different kinds of people such as boundary spanning functions and aging populations (Nimrod, 2018; Tams et al., 2014; Tarafdar et al., 2015c). Practically speaking, we are also beginning to see examples of phenomenon such as surveillance of individuals by employers, brought about by devices such as Fitbits (Yeung and Cevallos, 2017). Stress and anxiety that go hand in hand with such phenomenon, yet to be examined, can form a fertile are of new research as far as the level of the individual is concerned.

4. What is next or what can we be doing better as an area of research? Comments on emerging "dark side" areas and research techniques.

D'Arcy: Again, I will focus my responses to this question in the context of behavioral IS security research. Research on this topic can be improved in terms of theoretical drivers of both positive and negative security-related behaviors. As shown in recent reviews of the behavioral IS security literature (Cram et al., forthcoming; Hui et al., 2016; Moody et al., 2018), the work in this area has utilized a fairly limited set of theories from criminology, morality/ethics, psychology, and sociology. Namely, quite a bit of work has accumulated using theoretical perspectives such as deterrence/rational choice theory, neutralization theory, protection motivation theory (PMT), theory of reasoned action (TRA), theory of planned behavior (TPB), and the theory of cognitive moral development. While these theory bases have helped inform our understanding of behavioral IS security issues, it is clear that we still have a way to go. To this point, evidence continues to suggest that employee-related factors are at the heart of many security breaches, and so from both a theoretical and practical perspective, it can be argued that our understanding of the phenomenon is far from complete. It is time for the field to consider different theories above and beyond those that have been used extensively in behavioral IS security research (e.g., PMT, TPB) and to look at how theories can be combined to better understand the complex behavioral issues related to IS security.

Aside from the need for theoretical advances, there is a need for more advanced methodological approaches for studying behavioral IS security issues. A common approach in past studies has been to provide participants with hypothetical scenarios depicting, for example, an ISP non-compliance scenario and then asking respondents to rate their likelihood of engaging in the same behavior. This is a valid technique that has a history in the social sciences literature. Moreover, the scenario technique was necessitated, to some degree, by the difficulties that researchers experienced with trying to obtain actual security-related data (e.g., internal security breach incidents, logs of employee computing behaviors, etc.) from organizations. This situation remains today, as most organizations are hesitant to provide employee-related data related to IS security, for a variety of reasons. This point aside, there are limitations to the scenario approach that should be highlighted, particularly when scenarios are used to study negative security-related behavior. In such cases, it is assumed that participants can project themselves into the scenario situation (e.g., an ISP non-compliance behavior). The difficulty with this approach is that many acts of ISP non-compliance are committed by well-meaning employees who are simply trying to perform their jobs efficiently. In many cases such employees are stressed from security requirements (e.g., dealing with time pressure when makes them bypass a security protocol), which drives the ISP non-compliance behavior. It stands to reason that many participants would have difficulty projecting themselves into a hypothetical situation of ISP non-compliance—that is, pretending to be "bad person" doing "bad things." This places some limitations on the hypothetical scenario approach.

A methodological improvement would be a research design wherein participants are faced with ISP compliance/non-compliance decisions in situ. An example would be an experiment where the participant is presented with a security requirement that is likely to induce stress, and then the participant's behavior is evaluated; or, a longitudinal study wherein participants are dealing with excessive security requirements over time, to gauge whether they experience security fatigue, and then the outcomes of such fatigue can be evaluated. Obviously, conducting such studies is difficult and involves extensive resources, recruiting efforts, and, in some cases, one or more partner organizations. Obtaining partner organizations is likely a difficult endeavor for a single researcher or research team. Instead, such partnerships often necessitate the backing of a university research center and/or personal relationships between the researchers and partner organizations. In my own work, I have had some success in recruiting participants for longitudinal studies using online panels (e.g., MTurk and Qualtrics) (D'Arcy and Lowry, 2019; D'Arcy and Teh, forthcoming), so this is a potential means to bypass the partnering with organizations to obtain study participants. But these longitudinal studies required extensive coordination and the participants were well compensated.

In conclusion, I think the types of methodological advances that are needed in behavioral IS security research can only be attained through more extensive partnering with industry and/or conducting longitudinal studies. If a partnership is formed, there may be opportunities for more "natural experiments" wherein the researchers work with an organization to implement an actual security-related condition or program (e.g., a new phishing test or security training approach) and then they evaluate how employees responded to it over time. It is these types of realistic and longitudinal research designs that will help advance our understanding of behavioral IS security

issues in the future. Moreover, these more advanced and rigorous research designs can be applied to other areas in which "dark side" behaviors are being investigated.

Qahri-Saremi: *Emerging "dark sides" research areas:* As noted earlier in my response to the previous question, an important emerging area within "dark sides" of the digitization of the individual is the diminished user control in face of algorithmic intelligence, which presents a growing array of unintended and negative consequences for the users. What appears to be a recent case in point is the crash of Lion Air's "Boeing 737 MAX 8", one of Boeing's newest and most technologically advanced planes, in October 2018. The information from the flight data recorder, contained in a preliminary report by Indonesian crash investigators, documents "a fatal tug-of-war between man and machine, with the plane's nose forced dangerously downward more than two dozen times during the 11-minute flight. The pilots managed to pull the nose back up over and over until finally losing control, leaving the plane, Lion Air Flight 610, to plummet into the ocean at 450 miles per hour, killing all 189 people on board" (Glanz et al., 2018). Such subversion of user control vis-à-vis algorithmic intelligence is not limited to this one case.

Another case in point is the influence of algorithmic intelligence in the criminal justice system as a large number of U.S. states use a variety of intelligent risk-assessment algorithms to determine whether a prisoner should get a parole (Kehl et al., 2017). To do so, intelligent algorithms, owned by private tech-companies, scan prisoners' biographies to predict likelihood of their future criminal behavior (Walker, 2013), in a way that is both subtle and invisible to a human judge who has no access to how the algorithms make the decision, attributing a risk score to a prisoner (Demetis and Lee, 2018). To make it worse, it has been discovered that these algorithms could be biased against black defendants (Angwin et al., 2016). Besides the legal implications of such biases, what seems particularly troubling in such a case is the *diminished user control* over the algorithms that can have consequential effects on human lives (Demetis and Lee, 2018; Markus, 2015; Markus, 2017; Yoo, 2015). This subversion of user control in face of algorithmic intelligence is becoming far too common and exacerbating, as we observe in other cases such as automated stock trading, automated news filtering and production, self-driving cars, and job recruiting (Carlson, 2018; Constantiou and Kallinikos, 2015; Demetis and Lee, 2018; DeVito, 2017; Markus, 2017). This diminishing of user controls over *their* decisions and the consequences has become a new aspect of the digitization of the individual, which, at least in some contexts, can be troubling. Therefore, it is an important and emerging area of research within the dark-sides of the digitization of the individual.

Emerging research approaches: (I) Person-centered approaches - As a well-established and dominant approach in information systems research for decades, including the research on the dark sides of the digitization of the individual, the *variable-centered approach* focuses on the variables in a research model, rather than the individuals. This approach has drawn on pertinent statistical techniques, such as regression and structural equation modeling (SEM) to infer how the variance in outcome variables can be explained by the variances in exogenous variables in a research model (Meyer and Morin, 2016). A key characteristic of the variable-centered approach is its focus on capturing the interrelatedness (covariance-based relations) among a set of different variables and using this interrelatedness to infer about the underlying causes (or associations) of a specific phenomenon or behavior (Wang and Hanges, 2011). While following a variable-centered approach has been instrumental in understanding IS users' behaviors, revisiting two limitations underlying this approach can open up opportunities for a new research approaches

and thus new findings. First, variable-centered approach mainly considers the individuals (i.e., users) at the population (or sample) level without addressing the possible differences among the different subsets of individuals in the sample. Nonetheless, "not all individuals are created equal" as they mark different levels on different variables (some of which can be unobserved)—they have different profiles in terms of personality, beliefs, attitudes, emotions, and behaviors. Second, variable-centered analyses are limited in terms of the number of relations that can be addressed in one study. As a result, many of the plausible interrelations among variables in variable-centered studies are often overlooked due to the scope limitations. Nonetheless, "not all variables are created independent" as they can influence and moderate each other's effects on the behaviors of interest. A person-centered approach can address these two limitations and consequently, complement variable-centered findings.

The person-centered approach and its pertinent analysis techniques, such as latent profile analysis (LPA) (Muthén and Muthén, 1998-2015; Zyphur, 2009), strive to identify a typology of individuals, by taking into account their variations within a set of variables (Meyer et al., 2013). Unlike variable-centered approaches that focus on the role of specific variables, this approach acknowledges that variables can combine differently for some types of users than they do for others (Meyer and Morin, 2016; Meyer et al., 2013; Morin et al., 2016). Thus, rather than focusing on identifying the variables and per se and how they relate to each other in a population as a whole, the person-centered approach focuses on individuals to identify and compare unobserved subgroups (latent classes, prototypical profiles) of individuals with similar characteristics (Meyer et al., 2013; Zyphur, 2009). This enables researchers to capture the holistic, combined effects of multiple variables; and to control the effects of others in identifying typologies of users with respect to behaviors of interest. Consequently, recent calls have been issued for the inclusion of the person-centered approach in research *as a complementary approach* to be combined with variable-centered approaches (e.g., Gabriel et al., 2015; Meyer and Morin, 2016; Meyer et al., 2013; Morin et al., 2016; Wang and Hanges, 2011). The advantage of this combination is viewing a phenomenon of interest from two complementary perspectives, which can provide more comprehensive insights on the phenomenon under study (Meyer and Morin, 2016; Morin et al., 2011; Wang and Hanges, 2011; Zyphur, 2009). There is a paucity of person-centered research on the dark sides of the digitization of the individual, making it a ripe opportunity for future research in this area.

(II) Meta-Analysis - Given the recent growing focus on the dark sides of digitization of the individual, scholarly endeavors have resulted in a growing literature with a profusion of different variables that have been tested based on a variety of theoretical underpinnings in this area. This profusion and variety of findings can make consensus regarding important variables influencing the dark sides of digitization of the individual difficult to reach. Meta-analytical studies can be helpful in such a situation. Meta-analysis is a method for systematically reviewing a domain of scientific literature and quantitatively determining the significance and reliability of findings across studies in that literature (Eden, 2002). It has gained widespread recognition as an indispensable method for quantitatively integrating knowledge garnered in different empirical studies on a topic (Eden, 2002; He and King, 2008). As a result, meta-analysis is widely used across many disciplines, such as psychology (e.g., Chan et al., 2017), medicine (e.g., Hart et al., 2007), management (e.g., Eden, 2002; Kong et al., 2014), as well as information systems (e.g., Montazemi and Qahri-Saremi, 2015; Montazemi et al., 2012; Sharma and Yetton, 2007; Wu and Lederer, 2009), to extend knowledge by clarifying and synthesizing extant research findings (Eden, 2002). The paucity of meta-analytical studies on dark sides of the digitization of the

individual and the variety and profusion of empirical findings in this area render meta-analysis an instrumental technique for future research in this area.

Tarafdar: In my view, new dark side phenomenon should be examined, to cumulatively develop the literature in this area. For example, the phenomenon of the quantified self (Lupton, 2016) can lead to anxiety and social pressure as individuals struggle to manage the effects of data collected about the most personal and private aspects of their lives such as their food, physical activities and socialization (Barcena et al., 2014). Alongside these new phenomena IS scholars have the opportunity to use new types of data and methods to investigate them. To continue the example, data about the quantified self can be collected through devices such as applications on smartwatches and smartphones and over longitudinal phases (Pevnick et al., 2016). Such data can be triangulated with subjectively acquired data, to yield more robust findings.

Once again, looking at how technostress can be researched is helpful because it suggests a number of aspects (Tarafdar et al., 2019) of which I will briefly mention three. The first is the matter of measurement. The psychological stress literature has drawn from both psychological and physiological measures. However, such measures do not always correlate because their focus of measurements are different. Thus, I suggest pluralism and triangulation in measures. Specifically, for technostress, psychological measures can assess the subjective aspects such as challenge and threat techno-stressors, and psychological and behavioral outcomes. Physiological measures can study the short-term (blood pressure and hormones) or long-term (ulcer) strains (Tams et al., 2014). System use measures can capture the nature and extent of IS use. Second is the matter of design. Many dark side phenomena, including technostress, play out over time and thus longitudinal research designs are particularly helpful. The third is the matter of the research team. Given the complexity of dark side phenomenon, it is likely that research teams will need collaboration among different disciplines. In technostress research for example, IS researchers are collaborating with psychological stress researchers to address the conceptual scope of this phenomenon as demonstrated in recent publications (Stich et al., 2019; Tarafdar et al., 2019).

5. Conclusions

Overall, the panelists have shed light onto their own foci on dark sides of the Digitization of the Individual issues and charted the way for future research in this domain. It is noteworthy that even though each panelist has focused on a different dark-side area of research (IS security behaviors [D'Arcy], problematic and addictive use of technologies and loss of control over technology-mediated decisions [Qahri-Saremi], and technostress, loss of privacy and the blurring of work-life boundaries [Tarafdar], they presented consensus in terms of (1) the need to further study dark sides of the Digitization of the Individual, and (2) the potential and constant growth of phenomena that fall under this umbrella term. The variety of technologies the panelists have focused on is also noteworthy, ranging from work applications [D'Arcy], to social media and artificial intelligence [Qahri-Saremi], and to work technologies and fitness trackers [Tarafdar].

Lastly, the proposed methodological advancements (using more realistic security compliance experiments [D'Arcy], collecting data with fitness trackers or other objective system use measures [Tarafdar], and using a person center approach and meta-analytical techniques [Qahri-Saremi]) are informative; they can pave the way for innovative and impactful research in this domain.

Together, the broad and expending range of opportunities for research in this domain, the innovative methodologies proposed, and the broad and expanding set of technologies that have been weaved into our lives, make the dark side of the Digitization of the Individual a fruitful area for future research. The participation of the audience that attended the workshop in a lively follow up discussion also attests to the potential, importance, and impact of this research domain. We hence call for more research in this domain.

References

Addas, S. and Pinsonneault, A. (2018), "Email interruptions and individual performance: is there a silver lining?", *MIS Quarterly*, Vol. 42 No. 2**,** pp. 381-405.

Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016), "Machine bias: there's software used across the country to predict future criminals. And it's biased against blacks.", available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (accessed 10 March 2019).

Ayyagari, R. (2012), "An exploratory analysis of data breaches from 2005-2011: trends and insights", *Journal of Information Privacy and Security*, Vol. 8 No. 2**,** pp. 33-56.

Ayyagari, R., Grover, V. and Purvis, R. (2011), "Technostress: technological antecedents and implications", *MIS Quarterly*, Vol. 35 No. 4**,** pp. 831-858.

Barcena, M.B., Wueest, C. and Lau, H. (2014), "how safe is your quantified self?", available at: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/how-safe-is-your-quantified-self-14-en.pdf (accessed 10 March 2019).

Bata, H., Pentina, I., Tarafdar, M. and Pullins, E.B. (2018), "Mobile social networking and salesperson maladaptive dependence behaviors", *Computers in Human Behavior,* Vol. 81**,** pp. 235-249.

Carlson, M. (2018), "Automating judgment? Algorithmic judgment, news knowledge, and journalistic professionalism", *New Media & Society,* Vol. 20**,** pp. 1755-1772.

Chan, M.-P.S., Jones, C.R., Hall Jamieson, K. and Albarracín, D. (2017), "Debunking: a meta-analysis of the psychological efficacy of messages countering misinformation', *Psychological Science,* Vol. 28**,** pp. 1531-1546.

Chan, T.Y.H., Cheung, C.M.K. and Wong, R.Y.M. (forthcoming), "Cyberbullying on social networking sites: the crime opportunity and affordance perspectives", *Journal of Management Information Systems*.

Chen, A. and Karahanna, E. (2018), "Life interrupted: the effects of technology-mediated work interruptions on work and nonwork outcomes", *MIS Quarterly,* Vol. 42 No. 4**,** pp. 1023-1042.

Constantiou, I.D. and Kallinikos, J. (2015), "New games, new rules: big data and the changing context of strategy", *Journal of Information Technology,* Vol. 30**,** pp. 44-57.

Cram, A., D'Arcy, J. and Proudfoot, J. (forthcoming), "Seeing the forest and the trees: a meta-analysis of the antecedents of information security policy compliance", *MIS Quarterly*.

Cram, A., Proudfoot, J. and D'Arcy, J. (2019), When enough is enough: investigating the antecedents and consequences of information security fatigue.

D'Arcy, J., Gupta, A., Tarafdar, M. and Turel, O. (2014a), "Reflecting on the 'dark side' of information technology use", *Communications of the Association for Information Systems,* Vol. 35**,** pp. 109-118.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014b), "Understanding employee responses to stressful information security requirements: a coping perspective", *Journal of Management Information Systems,* Vol. 31 No. 2**,** pp. 285-318.

D'Arcy, J. and Lowry, P.B. (2019), "Cognitive-affective drivers of employees' daily compliance with information security policies: a multilevel, longitudinal study", *Information Systems Journal,* Vol. 29 No. 1**,** pp. 43-69.

D'Arcy, J., Herath, T., Yim, M.-S., Kichan, N. and Raghav, H.R. (2018), "Employee moral disengagement in response to stressful information security requirements: a methodological replication of a coping-based model", *AIS Transactions on Replication Research,* Vol. 4**,** pp. 1-17.

D'Arcy, J. and Teh, P.-L. (forthcoming), "Predicting employee information security policy compliance on a daily basis: the interplay of security-related stress, emotions, and neutralization", *Information & Management*.

Demetis, D. and Lee, A. (2018), "When humans using the IT artifact becomes IT using the human artifact", *Journal of the Association for Information Systems,* Vol. 19 No. 10**,** pp. 929-952.

DeVito, M.A. (2017), "From editors to algorithms: a values-based approach to understanding story selection in the facebook news feed", *Digital Journalism,* Vol. 5**,** pp. 753-773.

Eden, D. (2002), "From the editors: replication, meta-analysis, scientific progress, and AMJ's publication policy", *Academy of Management Journal,* Vol. 45**,** pp. 841-846.

Ernst and Young (2003), *Global Information Security Survey 2003*. New York, NY.

Gabriel, A.S., Daniels, M.A., Diefendorff, J.M. and Greguras, G. J. (2015), "Emotional labor actors: a latent profile analysis of emotional labor strategies", *Journal of Applied Psychology,* Vol. 100**,** pp. 863-879.

Glanz, J., Suhartono, M. and Beech, H. (2018), "In Indonesia Lion Air crash, black box data reveals pilots' struggle to regain control of doomed jet", *The New York Times*, 27 Nov 2018.

Goel, S. and Chengalur-Smith, I.N. (2010), "Metrics for characterizing the form of security policies", *The Journal of Strategic Information Systems,* Vol. 19 No. 4**,** pp. 281-295.

Hadlington, L. and Parsons, K. (2017), "Can cyberloafing and Internet addiction affect organizational information security?", *Cyberpsychology, Behavior, and Social Networking,* Vol. 20 No. 9**,** pp. 567-571.

Hart, R.G., Pearce, L.A. and Aguilar, M.I. (2007), "Meta-analysis: antithrombotic therapy to prevent stroke in patients who have nonvalvular atrial fibrillation", *Annals of Internal Medicine,* Vol. 146 No. 12**,** pp. 857-867.

He, J. and King, W.R. (2008), "The role of user participation in information systems development: implications from a meta-analysis", *Journal of Management Information Systems,* Vol. 25 No. 1**,** pp. 301-331.

Hui, K.L., Vance, A. and Zhdanov, D. (2016), "Securing digital assets", *MIS Quarterly, Research Curations*, available at:

https://www.misqresearchcurations.org/blog/2017/5/10/securing-digital-assets-1 (accessed 10 March 2019).

InformationWeek (2005), *U.S. Information Security Research Report 2005*, United Business Media.

Karadağ, E., Tosuntaş, Ş.B., Erzen, E., Duru, P., Bostan, N., Şahin, B. M., Çulha, İ. and Babadağ, B. (2015), "Determinants of phubbing, which is the sum of many virtual addictions: a structural equation model", *Journal of Behavioral Addictions,* Vol. 4 No. 2**,** pp. 60-74.

Kehl, D., Guo, P. and Kessler, S. (2017), "Algorithms in the criminal justice system: assessing the use of risk assessments in sentencing", Responsive Communities Initiative, Berkman Klein Center For Internet & Society, Harvard Law School, available at: https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf (accessed 10 March 2019).

Khansa, L., Kuem, J., Siponen, M. and Kim, S.S. (2017), "To cyberloaf or not to cyberloaf: the impact of the announcement of formal organizational controls", *Journal of Management Information Systems,* Vol. 34 No. 1**,** pp. 141-176.

Koay, K.Y. (2018), "Workplace ostracism and cyberloafing: a moderated-mediation model", *Internet Research,* Vol. 28 No. 4**,** pp. 1122-1141.

Kong, D.T., Dirks, K. and Ferrin, D. (2014), "Unterpersonal trust within negotiations: meta-analytic evidence, critical contingencies, and directions for future research", *Academy of Management Journal,* Vol. 57 No. 5**,** pp. 1235-1255.

Lowry, P.B. and Moody, G.D. (2015), "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies", *Information Systems Journal,* Vol. 25**,** pp. 433-463.

Lupton, D. (2016), *The Quantified Self*, John Wiley & Sons.

Maier, C., Laumer, S., Weinert, C. and Weitzel, T. (2015), "The effects of technostress and switching stress on discontinued use of social networking services: a study of facebook use", *Information Systems Journal*, Vol. 25 No. 3, pp. 275-308.

Markus, M.L. (2015), "New games, new rules, new scoreboards: the potential consequences of big data", *Journal of Information Technology,* Vol. 30 No. 1**,** pp. 58-59.

Markus, M.L. (2017), "Datification, organizational strategy, and is research: what's the score?", *The Journal of Strategic Information Systems,* Vol. 26 No. 3**,** pp. 233-241.

Matt, C., Trenz, M., Cheung, C. and Turel, O. (forthcoming), "The digitization of the individual: conceptual foundations and opportunities for research", *Electronic Markets*.

Mazmanian, M., Orlikowski, W.J. and Yates, J. (2013), "The autonomy paradox: the implications of mobile email devices for knowledge professionals", *Organization Science,* Vol. 24 No. 5**,** pp. 1337-1357.

McHugh, B.C., Wisniewski, P., Rosson, M.B. and Carroll, J.M. (2018), "When social media traumatizes teens: the roles of online risk exposure, coping, and post-traumatic stress", *Internet Research,* Vol. 28 No. 5**,** pp. 1169-1188.

Meyer, J.P. and Morin, A.J. (2016), "A person-centered approach to commitment research: theory, research, and methodology", *Journal of Organizational Behavior,* Vol. 37 No. 4**,** pp. 584-612.

Meyer, J.P., Stanley, L.J. and Vandenberg, R.J. (2013), "A person-centered approach to the study of commitment", *Human Resource Management Review,* 23**,** pp. 190-202.

Montazemi, A.R., Pittaway, J.J., Qahri-Saremi, H. and Wei, Y. (2012), "Factors of stickiness in transfers of know-how between MNC units", *Journal of Strategic Information Systems,* Vol. 21 No. 1**,** pp. 31-57.

Montazemi, A.R. and Qahri-Saremi, H. (2015), "Factors affecting adoption of online banking: a meta-analytic structural equation modeling study", *Information & Management,* Vol. 52 No. 2**,** pp. 210-226.

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a unified model of information security policy compliance", *MIS Quarterly,* Vol. 42 No. 1, pp. 285-311.

Morin, A.J., Meyer, J.P., Creusier, J. and Biétry, F. (2016), "Multiple-group analysis of similarity in latent profile solutions", *Organizational Research Methods,* Vol. 19**,** pp. 231-254.

Morin, A.J., Morizot, J., Boudrias, J.-S. and Madore, I. (2011), "A multifoci person-centered perspective on workplace affective commitment: a latent profile/factor mixture analysis", *Organizational Research Methods,* Vol. 14**,** pp. 58-90.

Muthén, L.K. and Muthén, B.O. (1998-2015), *Mplus User'S Guide,* Los Angeles, CA, Muthén & Muthén.

Neff, G. and Nagy, P. (2018), "Agency in the digital age: using symbiotic agency to explain human–technology interaction", in Papacharissi, Z. (Ed.), *A Networked Self And Human Augmentics, Artificial Intelligence, Sentience.* Routledge.

Nimrod, G. (2018), "Technostress: measuring a new threat to well-being in later life", *Aging & Mental Health,* Vol. 22 No. 8**,** pp. 1080-1087.

Ollier-Malaterre, A., Rothbard, N.P. and Berg, J. (2013), "When worlds collide in cyberspace: how boundary work in online social networks impacts professional relationships", *Academy of Management Review,* Vol. 38 No. 4**,** pp. 645-669.

Persily, N. (2017), "The 2016 US election: can democracy survive the Internet?", *Journal of Democracy,* Vol. 28**,** pp. 63-76.

Pevnick, J.M., Fuller, G., Duncan, R. and Spiegel, B.M. (2016), "A large-scale initiative inviting patients to share personal fitness tracker data with their providers: initial results", *PLoS ONE,* Vol. 11 No. 11**,** pp. E0165908.

Piszczek, M., Pichler, S., Turel, O. and Greenhaus, J. (2016), "The information and communication technology user role: implications for the work role and inter-role spillover", *Frontiers In Psychology,* Vol. 7**,** pp. 1-15.

Ponemon Institute (2016), Managing Insider Risk Through Training and Culture, Ponemon Institute LLC.

Porter, G. and Kakabadse, N.K. (2006), "HRM perspectives on addiction to technology and work", *Journal of Management Development,* Vol. 25 No. 6**,** pp. 535-560.

Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J. and Courtney, J.F. (2013), "Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of protection-motivated behaviors", *MIS Quarterly,* Vol. 37 No. 4**,** pp. 1189-1210.

Power, R. (2003), "2003 CSI/FBI Computer Crime and Security Survey", *Computer Security Issues and Trends,* 9.

PwC (2016), *The Global State of Information Security Survey 2016*.

Qahri-Saremi, H. and Turel, O. (2016), "School engagement, information technology use, and educational development: an empirical investigation of adolescents", *Computers & Education,* Vol. 102**,** pp. 65-78.

Ragu-Nathan, T.S., Tarafdar, M., Ragu-Nathan, B.S. and Tu, Q. (2008), "The consequences of technostress for end users in organizations: conceptual development and empirical validation", *Information Systems Research,* Vol. 19 No. 4**,** pp. 417-433.

Salo, M., Pirkkalainen, H. and Koskelainen, T. (forthcoming), "Technostress and social networking services: explaining users' concentration, sleep, identity, and social relation problems", *Information Systems Journal*.

Sarker, S., Ahuja, M. and Sarker, S. (2018), "Work-life conflict of globally distributed software development personnel: an empirical investigation using border theory", *Information Systems Research,* Vol. 29 No. 1**,** pp. 103-126.

Schultz, E.E. (2002), "A framework for understanding and predicting insider attacks", *Computers & Security,* Vol. 21 No. 6**,** pp. 526-531.

Sharma, R. and Yetton, P. (2007), "The contingent effects of training, technical complexity, and task interdependence on successful information systems implementation', *MIS Quarterly,* Vol. 31 No. 2**,** pp. 219-238.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers & Security,* Vol. 24 No. 2**,** pp. 124-133.

Stich, J., Tarafdar, M., Stacey, P. and Cooper, C.L. (2019), "Appraisal of email use as a source of workplace stress: a person-environment fit approach", *Journal of the Association for Information Systems,* Vol. 20 No. 2, pp. 132-160.

Tams, S., Hill, K., De Guinea, A.O., Thatcher, J. and Grover, V. (2014), "Neurois-alternative or complement to existing methods? illustrating the holistic effects of neuroscience and self-reported data in the context of technostress research", *Journal of the Association for Information Systems,* Vol. 15 No. 10**,** pp. 723-753.

Tarafdar, M., Cooper, C.L. and Stich, J.F. (2019), "The technostress trifecta-techno eustress, techno distress and design: theoretical directions and an agenda for research", *Information Systems Journal,* Vol. 29 No. 1**,** pp. 6-42.

Tarafdar, M., Darcy, J., Turel, O. and Gupta, A. (2015a), "The dark side of information technology", *MIT Sloan Management Review,* Vol. 56 No. 2**,** pp. 600-623.

Tarafdar, M. and Davison, R.M. (2018) "Research in information systems: intra-disciplinary and inter-disciplinary approaches", *Journal of the Association for Information Systems*, Vol. 19, No. 6, pp. 523-551.

Tarafdar, M., Gupta, A. and Turel, O. (2013), "The dark side of information technology use", *Information Systems Journal,* Vol. 23 No. 3**,** pp. 269-275.

Tarafdar, M., Gupta, A. and Turel, O. (2015b), "Editorial: special issue on 'dark side of information technology use': an introduction and a framework for research", *Information Systems Journal,* Vol. 25 No. 3**,** pp. 161-170.

Tarafdar, M., Pullins, E.B. and Raghu-Nathan, B. (2014), "Examining impacts of technostress on the professional salesperson's behavioural performance", *Journal of Personal Selling and Sales Management,* Vol. 34 No. 1**,** pp. 51-69.

Tarafdar, M., Pullins, E.B. and Ragu-Nathan, T.S. (2015c), "Technostress: negative effect on performance and possible mitigations", *Information Systems Journal,* Vol. 25 No. 2**,** pp. 103-132.

Tarafdar, M., Tu, Q., Ragu-Nathan, B.S. and Ragu-Nathan, T.S. (2007), "The impact of technostress on role stress and productivity", *Journal of Management Information Systems,* Vol. 24 No. 1**,** pp. 301-328.

Tarafdar, M., Tu, Q., Ragu-Nathan, T.S. and Ragu-Nathan, B.S. (2011), "Crossing to the dark side: examining creators, outcomes, and inhibitors of technostress", *Communications of the ACM,* Vol. 54 No. 9**,** pp. 113-120.

Turel, O. (2017), "Organizational deviance via social networking site use: the roles of inhibition, stress and sex differences", *Personality and Individual Differences,* Vol. 119**,** pp. 311-316.

Turel, O. and Bechara, A. (2016), "Social networking site use while driving: ADHD and the mediating roles of stress, self-esteem and craving", *Frontiers In Psychology,* Vol. 7.

Turel, O. and Bechara, A. (2017) "Effects of motor impulsivity and sleep quality on swearing, interpersonally deviant and disadvantageous behaviors on online social networking sites", *Personality and Individual Differences,* Vol. 108**,** pp. 91-97.

Turel, O. and Bechara, A. (forthcoming), "Little video-gaming in adolescents can be protective, but too much is associated with increased substance use", *Substance Use & Misuse*.

Turel, O., Poppa, N. and Gil-Or, O. (2018), "Neuroticism magnifies the detrimental association between social media addiction symptoms and wellbeing in women, but not in men: a three-way moderation model", *Psychiatric Quarterly,* Vol. 89 No. 3**,** pp. 605-619.

Turel, O. and Qahri-Saremi, H. (2016), "Problematic use of social networking sites: antecedents and consequence from a dual system theory perspective", *Journal of Management Information Systems,* Vol. 33 No. 4**,** pp. 1087-1116.

Turel, O. and Qahri-Saremi, H. (2018), "Explaining unplanned online media behaviors: dual-system theory models of impulsive use and swearing on social networking sites", *New Media & Society*, Vol. 20 No. 8**,** pp. 3050-3067.

Turel, O., Romashkin, A. and Morrison, K.M. (2016) "Health outcomes of information system use lifestyles among adolescents: videogame addiction, sleep curtailment and cardio-metabolic deficiencies", *PLoS ONE,* Vol. 11 No. 5**,** pp. E0154764.

Turel, O., Romashkin, A. and Morrison, K.M. (2017), "A model linking video gaming, sleep quality, sweet drinks consumption and obesity among children and youth", *Clinical Obesity,* Vol. 7 No. 4**,** pp. 191-198.

Turel, O. and Serenko, A. (2010), "Is mobile email addiction overlooked?", *Communications of the ACM,* Vol. 53 No. 5**,** pp. 41-43.

Turel, O., Serenko, A. and Bontis, N. (2011), "Family and work-related consequences of addiction to organizational pervasive technologies", *Information & Management,* Vol. 48 No. 2-3**,** pp. 88-95.

Vaghefi, I. and Qahri-Saremi, H. (2017) "From IT addiction to discontinued use: a cognitive dissonance perspective", *Proceedings of the 50th Hawaii International Conference on System Sciences, Big Island, Hawaii, 4-7 January 2017*.

Vaghefi, I. and Qahri-Saremi, H. (2018), "Personality predictors of IT addiction", *Proceedings of the 51st Hawaii International Conference on System Sciences, Big Island, Hawaii, 3-6 January 2017*.

Venkatesh, V., Sykes, T.A., Chan, F.K.Y., Thong, J.Y.L. and Hu, P.J.-H. (forthcoming), "Children's internet addiction, family-to-work conflict, and job outcomes: a study of parent-child dyads", *MIS Quarterly*.

Walker, J. (2013), "State parole boards use software to decide which inmates to release", *Wall Street Journal*, 11 October 2013.

Wang, M. and Hanges, P.J. (2011), "Latent class procedures: applications to organizational research", *Organizational Research Methods,* Vol. 14 No. 1**,** pp. 24-31.

Wu, J. and Lederer, A. (2009), "A meta-analysis of the role of environment-based voluntariness in information technology acceptance", *MIS Quarterly,* Vol. 33 No. 2**,** pp. 419-432.

Yeung, D. and Cevallos, A. S. (2017), "Using wearable fitness devices to monitor more than just fitness", *Scientific American*, available at: Https://Blogs.Scientificamerican.Com/Observations/Using-Wearable-Fitness-Devices-To-Monitor-More-Than-Just-Fitness/ (accessed 5 March 2019).

Yin, P., Ou, C.X.J., Davison, R.M. and Wu, J. (2018), "Coping with mobile technology overload in the workplace", *Internet Research,* Vol. 28 No. 5**,** pp. 1189-1212.

Yoo, Y. (2015), "It is not about size: a further thought on big data", *Journal of Information Technology,* Vol. 30 No. 1**,** pp. 63-65.

Young, K. (2017), *Internet Addiction Test (IAT),* Wood Dale, IL, Stoelting.

Young, K.S. and Case, C.J. (2004), "Internet abuse in the workplace: new trends in risk management", *Cyberpsychology & Behavior,* Vol. 7 No. 1**,** pp. 105-111.

Zakrzewski, C. (2016), "The key to getting workers to stop wasting time online", *The Wall Street Journal*, 13 March 2016.

Zyphur, M.J. (2009), "When mindsets collide: switching analytical mindsets to advance organization science", *The Academy of Management Review,* Vol. 34 No. 4**,** pp. 677-688.