Pers Ubiquit Comput
DOI 10.1007/s00779-016-0938-4

ORIGINAL ARTICLE

Exploring the relationship between impulsivity and decision-making on mobile devices

Debora Jeske[1,2] · **Pam Briggs**[2] · **Lynne Coventry**[2]

Received: 31 March 2015 / Accepted: 12 February 2016

Abstract Mobile devices offer a common platform for both leisure and work-related tasks, but this has resulted in a blurred boundary between home and work. In this paper, we explore the security implications of this blurred boundary, both for the worker and the employer. Mobile workers may not always make optimal security-related choices when "on the go" and more impulsive individuals may be particularly affected as they are considered more vulnerable to distraction. In this study, we used a task scenario, in which 104 users were asked to choose a wireless network when responding to work demands while out of the office. Eye-tracking data was obtained from a subsample of 40 of these participants in order to explore the effects of impulsivity on attention. Our results suggest that impulsive people are more frequent users of public devices and networks in their day-to-day interactions and are more likely to access their social networks on a regular basis. However, they are also likely to make risky decisions when working on-the-go, processing fewer features before making those decisions. These results suggest that those with high impulsivity may make more use of the mobile Internet options for both work and private purposes, but they also show attentional behavior patterns that suggest they make less considered security-sensitive decisions. The findings are discussed in terms of designs that might support enhanced deliberation, both in the moment and also in relation to longer term behaviors that would contribute to a better work–life balance.

Keywords Impulsivity · Visual processing · Cyber-security · Social networks · Work–life balance · Mobile working

1 Introduction

Mobile working is now commonplace, thanks in part to the widespread availability of public wireless networks, the growth in companies prepared to offer remote working [5] and the rise of the smartphone as a common platform for both leisure and work activities [25]. The result is a blurring of the relationship between home and work, most directly affecting the time spent on work or home tasks [6]. The advantage to the *worker* is that it offers them increased temporal and geographic flexibility and connectedness, but there are also disadvantages in terms of increased pressure, perceived or real, to be available for work around the clock and consequent feelings of stress and exhaustion [17]. The advantage to the *employer* is a more responsive, agile and available workforce and the opportunity to exert greater organizational control [38], but there is also a cost. Employers tend to underestimate the time workers spend on their mobiles and, in particular, underestimate time spent on social media [41]. Such flexible "anytime, anyplace" working on a mobile device can quickly become "all the time and everywhere". This universal work mode can also compromise security, with serious implications for both the worker and for the employer, and it is this issue that is explored in the current study.

✉ Pam Briggs
p.briggs@northumbria.ac.uk

[1] Business School, Edinburgh Napier University, 219 Colinton Road, Edinburgh EH14 1DJ, UK

[2] Department of Psychology, Northumbria University, Northumberland Road, Newcastle upon Tyne NE1 8ST, UK

Published online: 01 July 2016

1.1 Mobile working and the work–life boundary

Prior literature exploring mobile communication technologies as tools that increase work–life balance and break down the barriers between work and home [25, 65, 66, 69] suggests that both positive and negative outcomes may result. In a large-scale survey of 1388 individuals from 845 Australian households [65], the mobile phone was predominantly seen to be a social tool, but there was clear evidence of its increasing use as a work tool, particularly by the men in the sample. One of the main functions of the mobile phone was for "micro-coordination of family arrangements and work schedules" [65]—essentially reducing the rigidity of plans and allowing both work and home arrangements to be renegotiated at will. Note, however, that this micro-coordination was seen as a positive aspect to phone use and was associated with a significant proportion of respondents believing that the mobile had helped to balance their family and working lives. The same authors also made use of the "family strains and gains scale" [43] that measures ways that job-related stresses might transfer to the family and vice versa. They note that, contrary to popular belief, the work–family spillover was not significantly related to mobile phone use, but reflected other job characteristics (such as total hours worked). There was, however, clear evidence of the erosion of boundaries between home and work life, as for example, when both men (51 %) and women (31 %) chose to use their mobile phone to talk with their work colleagues while on holiday [65]. The use of work-related communication technologies outside work has also been shown to increase perceived work–life conflict [69] and raise concerns about technostress associated with the pervasive and near-continual use of organizational IT systems and the effect this has on health and work–life balance [59].

Between 2004 and 2008, there was a marked shift in the ways in which individuals would exploit the interoperability of various portable devices; and by the end of that period, it was common to connect to the Internet for both work and personal activities, for example when travelling or when in cafes or bars [9]. Today, it has become commonplace for employees to use the same social media sites to interact with friends, family and colleagues, creating a collision between personal and professional identities. The use of a common platform that can "collapse" identities in this way can result in a worker being careless in their demarcation or segregation of home and work activities which in turn can lead to information from one environment "leaking" into another. Thus, an employee may inadvertently reveal inappropriate personal information to their colleagues or sensitive, protected company information to their friends and family. A second factor is that the device itself may be vulnerable. Smartphones are typically armed with their own security systems. They can seamlessly load security updates or run maintenance checks, run virus screens in the background, and offer information alerts, but despite this, there are known security problems associated with being "always connected" [37]. Not surprisingly then, employers are under pressure to enhance their mobile-based security and authentication policies and procedures [53]. Employers increasingly utilize mobile device management and bring your own device (BYOD) policies to ensure that their mobile workers do not introduce new threats to workplace security. However, past evidence has shown that workers find it difficult to adhere to security policies, even within the workplace (see various reports on compliance issues by [3]). How much more difficult is it, then, to make optimal security decisions from a home or leisure environment when the same device is used for home and work activities. As a result, the distinction between home and work activities can become blurred, making it more challenging for users to adhere to company security policies under such circumstances.

There are a number of factors at play here. Firstly, the mobile worker must deal with increased task complexity, mastering not only the primary task itself, which can be challenging [48] but also gaining mastery of a device that has not necessarily been optimized to the task as well as dealing with any mobile services used in performance of that primary task. Secondly, the mobile worker may face a wide range of distractions (games, music, shopping and gambling) that are only a click away. Thirdly, the mobile worker may feel time pressure to submit work or reply to an e-mail even though they are operating in an insecure environment—such as a café with an open wireless network. In such a complex space, certain personality variables may also influence the extent to which any user can fully attend to the information most relevant to security-based decision-making. In particular, the *impulsive* individual may find it more difficult to prioritize security concerns, given that they may have difficulty to maintain focus and may be more impatient to get on with the primary task at hand. These personality issues are dealt with more detail in Sect. 1.3 below.

1.2 Mobile security

Mobile security has been a known issue for HCI for some time, with many of the published studies focusing on easier smartphone authentication [14]; or means to reduce unauthorized access [46]. In short, much of the HCI work has been focused upon more usable means of protecting the smartphone user. A new, broader focus on smartphone security has come into play with the rise of BYOD practices in the work environment, and the increasing awareness that organizational as well as personal data are at risk

from everyday insecure practices in mobile phone use [56]. Perhaps surprisingly, users are relatively unaware of the security challenges they face while conducting sensitive exchanges on a mobile device [31], believing that smartphone exchanges are generally less risky than those made on a laptop. This is interesting considering the frequency with which people will use smartphones to download apps, conduct e-mail or connect to an unsecured wireless network while travelling.

In our own studies of BYOD security, we have adopted a "security by design" approach, seeking to develop a "choice architecture" that will seamlessly nudge users toward secure decision-making. Such an approach builds upon the work of Thaler and Sunstein [60] and also on the work of Kahneman [34], who describes the importance of two cognitive systems in his 2011 text "Thinking, fast and slow". There are interesting design opportunities afforded by system 1—the "faster" of the two cognitive systems which operates quickly and with little or no cognitive effort or sense of voluntary control. In particular, it is possible to develop design nudges that support more secure decision-making in a relatively effortless way, by simply changing menu order or color-coding the choices [10] (e.g., in the case of wireless network selection). Such design nudges have been employed to great effect in the privacy space, where users are often thoughtless in their disclosure of sensitive information [1], but their use has been relatively limited for mobile security, which, as we have seen is becoming a critical issue. What is also interesting, for the current study, is the role that individual differences may come into play. Are some people less able or willing to engage system 2, i.e., reluctant to take a deliberative, analytical approach to managing their mobile security? Certainly deliberation would seem to be an important consideration when considering cyber-security practice outside of the workplace, given, for example, the finding that users who take a deliberative approach to mobile security (reading software policies and checking for trust kitemarks) are much less susceptible to malware [8].

1.3 Personality and security-related behavior

Certain personality variables can help predict security-related behavior on mobile devices and social media. They may shape the values users adopt, the types of information they share and the people with whom they share this information. In addition, just as personality can shape behavior, so conversely, behavior can be used to indicate the presence of certain personality traits. We propose that this relationship holds true in the security space, where compliance with security policy, non-responses to security messages and/or security prompts are mediated by stable characteristics of the users themselves. This approach recognizes that personality sits alongside knowledge and experience, cognitive capacities, heuristics and biases—all of which shape the interpretation of security messages and the willingness of the user to commit to secure practices.

A few general examples demonstrate this point. For example, introverts engage in more cautious online behavior, and both extroversion [55] and shyness [20] influence Internet behavior and search activities [11, 20, 26] as well as privacy and security risk perceptions [55]. Other personality traits that have been shown to influence security practices include "big-five" factors (such as neuroticism, openness to experience, conscientiousness) as well as self-efficacy. For example, a correlation has been found between neuroticism scores and susceptibility to phishing e-mails [27]. Social media users who rank high in openness to experience also set fewer privacy settings, making them more vulnerable to attacks [27]. Conscientiousness positively influences information security managers' attitudes toward technical as well as organizational activities associated with information security and security compliance, and greater security self-efficacy is associated with greater security efforts [57].

Personality can also moderate the effectiveness of security campaigns. For example, users ranking high on agreeableness are more likely to improve their security behavior when security advice incorporates a moral, regret or feedback component [35]. However, these behavioral change incentives were not as effective for those users who also rank high in terms of openness to experience [35]. Such findings therefore support the idea that personality can influence security behaviors, in terms of the attention users pay to security interfaces, and the types of advice they are likely to follow.

This paper focuses on the relationship between *impulsivity* and security-related decision-making. Impulsivity is the tendency of individuals to act in the moment [42]. More impulsive individuals find it difficult to sustain attention, which means they deliberate less when making decisions [28, 32, 58] and often miss information [18]. Impulsive individuals are also more likely to focus on potential rewards, pay less attention to possible negative outcomes of decisions [44] and also discount the value of delayed rewards [68]. They may also be more fixed on specific choices and less willing to change their decisions in response to different incentives [22]. Finally, impulsivity may also indicate a poorer ability to separate personal and work time effectively when using mobile devices [17], which may result in problems in maintaining a reasonable work–life balance.

The implications for decision-making when balancing competing demands, including security-related behaviors, are manifold. Impulsive individuals may not act on advice

at a given time because they do not see the immediate benefit of doing so or because they find it difficult to adapt their behavior to changing circumstances (exhibiting choice fixedness as suggested by [22]). More impulsive users may also prioritize immediate and gratifying outcomes over long-term considerations such as security. This is important since meeting security requirements is rarely the users' primary focus or task as the user's cognitive resources are limited [3]. This means, the user may have insufficient resources to respond to security requests when he or she is already working on another task. The security risks are compounded if greater impulsivity coincides with a tendency to be more trusting [55]. This would explain why impulsive individuals are also more likely to respond to phishing e-mails and are less attentive to the cues that would alert them to a scam [50]. In addition, past work has shown that the use of mobile technology and successful management of work–life boundaries is influenced by their ability to respond to demands from home and their level of self-control [19]. This provides further support for the potential role of impulsivity in relation to boundary management.

Not surprisingly then, there is also evidence that impulsivity is linked to poorer self-regulation and sensation seeking. This again may articulate itself in form of problematic Internet use [5]. This can extend to the workplace: In one study, employees with lower self-control (a measure that includes impulsivity) also admitted that they would be more likely to violate cyber-security policy [29]. Given the poor self-regulation aspect and processing of information, more impulsive individuals may not necessarily be aware of their poor information processing or the fact that they are compromising their privacy.

1.4 Rationale and goals of current study

A number of personality and contextual factors can influence security behaviors. These are affected by work-life demands but may not accounted for by the organisation [24]. Impulsiveness is one of those factors that have been considered in relation to self-regulation and problematic Internet use [5] and cyber-security policy compliance [29]. Impulsiveness may increase the susceptibility of an individual to distractions originating from the persuasive pull of mobile communication technologies and the availability of social networks. However, relatively little is known about how impulsivity might affect security decision-making outside of the work environment where users are more likely to be dealing with multiple and diverse demands. Impulsive employees are probably less tolerant of delays in their workflow, less able to resist frequent status checking of their mobiles and more easily distracted—all of which might mean that they are also more likely to blur their work–life boundaries and render them more vulnerable to security attacks.

The first study goal was to examine whether impulsivity was related to the deliberation of available wireless options, as poor deliberation could lead to insecure decision-making. Researchers have previously utilized eye-tracking technology and made use of gaze paths and fixation points to explore the users' interaction with security indicators within web browsers [12]. In our study, we predict that individuals scoring high on impulsivity process fewer features than those scoring low on impulsivity. More impulsive people may also struggle to focus on the task at hand, resulting in riskier decision-making (linked to poor self-regulation during the visual processing of materials).

Hypothesis 1 Impulsivity is a negative predictor of the number of features processed.

The second goal was to expand on past work on poor self-regulation and impulsivity by considering the relationship between impulsivity and privacy concern. As noted above, impulsive individuals exhibit more problematic behaviors online and are more prone to sensation seeking [5]. This suggests that more impulsive individuals may be less concerned about privacy, in part because they do not attend to the longer term consequences of their actions. This may lead to privacy breaches that could affect their employers' and their own personal data security.

Hypothesis 2 Impulsivity is negatively correlated with privacy concern.

The third goal was to consider the possibility that more impulsive individuals may be less able to maintain focus and stay engaged with one activity in the presence of other distracting and less demanding activities. They may show a greater tendency to pick up mobile devices to access social media sites, as suggested by past work linking impulsivity and Internet addiction [39]. We are not suggesting that more impulsive individuals are less engaged or interested. Rather, impulsive individuals may be more readily enticed and persuaded to use their mobiles to connect to the Internet via public wireless networks in order to check for updates and review the status of their social networks. As noted earlier, impulsive individuals are more easily distracted [28, 32, 58]. This may translate into a greater tendency to access social media and other mobile distractions which in turn, might leave them vulnerable to security risks including credit card fraud or phishing, as they may engage in less careful screening of information sent to them. We therefore propose that impulsivity is connected to how frequently individuals use mobile devices to access public

wireless networks and to check their social network account.

Hypothesis 3 Impulsivity is positively correlated with mobile device use and social media access.

2 Methods

2.1 Participants

Social science students were recruited by posting a message on a dedicated university online recruitment portal. Students are a relevant sample in this case because they rely on and make assumptions about the security of university infrastructure and their publicly available open access services [36], but they exhibit limited awareness of the security issues involved with online transactions [54]. Students are also an interesting population as they have concerns about work–life balance; concerns that may even be more pronounced if they combine family and work responsibilities with part-time study and raising a family. According to a report Higher Education Careers Services Unit [45], 36 % of students in the UK were part-timers in 2007–2008. Part-time students are often older and work while studying. Many students experience conflicting prioritiesas a result of having no experience or strategies to manage work–life conflicts, but also due to institutional culture and ethos in higher education [40].

All university students could earn research credits for their respective programs. The first forty participants were recruited in Autumn 2013 and completed the task in a laboratory setting that enabled us to also collect eye-tracking data. The remaining participants were given an online version of the task in Spring 2014. All instructions and materials were identical in both data collection phases and no significant effects of online versus off-line task completion were observed. One color-blind participant was excluded from the eye-tracking subsample. The final sample ($N = 104$) comprised 46 males and 53 female students with an average age of 21 years (MN = 21.61, SD = 4.84, range 18–40; 5 missing values). Half of the participants used the Internet at home ($n = 54$, 51.9 %) or both at work and home ($n = 46$, 44.2 %).

2.2 Procedure

Upon completion the appropriate consent forms, all participants were given the following scenario: *You have an hour to submit some urgent work and decide to go to a public café to connect to the Internet using one of several available wireless connections*. Keeping this scenario in mind, they were then presented with five screens. Each screen offered six network options. Participants had to select one of the network options for each screen. The 41 participants were monitored discretely with an eye tracker while they explored each screen on a monitor. Following the selection of their choices, all participants were asked to complete a follow-up questionnaire about their personality, their use of various devices and their social and wireless networks. The questionnaire concluded with demographics and the debrief statement about the study.

2.3 Materials

The network options were presented on five screens similar to an Android default Wi-Fi selection screen. Each screen provided six networks from which participants had to choose one. The five screens themselves varied in terms of how the network options were presented to participants (using color coding, ordering of networks and presence of padlocks) and the behavioral effects of these different "nudges" are presented in [10, 61]. To avoid familiarity effects, network names were replaced with randomly generated network names. Screens were presented in a random order to participants. In this paper, we report how impulsivity affects attention to information when making decisions and use of devices and social media.

2.4 Measures

Behavioral and self-report measures are detailed below.

2.4.1 Attention score

The first set of outcomes referred to data obtained from eye tracking. Tobii Studio 3.0.2 was used to collect data about the frequency with which individuals looked at the various areas of interest (AOIs), fixation counts, time required per screen and various other indicators of visual processing. An X120 eye tracker was located directly beneath the monitor. This setup does not require the participant to wear any special equipment; it is just necessary to stay within the range of the device. Using the software, the researchers drew 12-specific AOIs using the graphics tools (network label to the left, signal and padlock to the right) for each of the five screen variations, resulting in a total of 60 AOIs (thus, using the same size and parameters for all participants when they were looking at one of the AOIs). The time participants took to make their choices was not restricted. In our study, the eye movements of every participant in the subsample were carefully examined to detect and compute the total number of screen features (e.g., number of options and symbols) each participant processed from each screen while making decisions. In order to do this, the recordings were slowed down and visually

inspected by a research assistant who counted how many features each person processed. The results were summed across all screens to generate the processing score. On average, participants appeared to have visually attended to most but not all of the 12 AOIs on each screen (MN = 9.28, SD = 1.11).

Another important variable was the percentage provided for sampling effectiveness by Tobii Studio (on a scale of 1–100 %). The program generates this measure ("samples") as a means of determining the quality of the eye recording. It gives a sense of the number of valid gaze points in the recording, if not necessarily the accuracy of the recording. A researcher was present to ensure that all participants were focused on the screen and not distracted. Slight misalignment can lead to specific gazing patterns not being counted, especially when the area of interest is small. Using the data from Tobii, the visual processing data were examined for the first 10-s period during which participants picked their preferred network option (participants usually started to revisit the same AOIs after this point). Our coding of AOIs scanned within 10 s strongly correlated with the statistics produced by the Tobii Studio for AOIs scanned by participants ($r = .812$, $p < .001$). A variety of measures were used to assess personality, social media and wireless network use in the follow-up questionnaire. In some cases, the scales were shortened to reduce the length of the follow-up questionnaires and reduce the likelihood of participant of fatigue and disengagement.

2.4.2 *Impulsivity*

Four items from the ten-item Diminished Impulse Control subscale (part of the Online Cognition scale) were used to assess impulsivity [13]. This scale was selected because it had been specifically designed as a means to assess both cognitive and behavioral control in relation to online activities and decision-making. This measure has also been used in other online research [20, 26, 31, 48]. Only four items were selected from the list of ten for two reasons: One was related to practicality (we aimed to keep the follow-up questionnaire reasonably short) and the other concerned the content of the items as these particular items captured problematic Internet use that is linked to impulsivity [see original scale information in 13]. The four items were: (1) "I use the Internet more than I ought to." (2) "People complain that I use the Internet too much." (3) "I never stay on longer than I had planned." (4) "Even though there are times when I would like to, I can not cut down on my use of the Internet." The third item was reverse-coded. The response scale ranged from (1) strongly disagree to (5) strongly agree. We decided to use five response options in line with other measures. The reverse-coded item was excluded due to poor reliability. Impulsivity score was computed as the average of the remaining items ($\alpha = .643$, MN = 3.26, SD = .77). This gave us a range of responses between 1 and 5 with higher scores indicating greater impulsivity.

2.4.3 *Privacy concern*

Two items were used to measure privacy concern [7]. The original scale had included questions not statements, each with response options on a five-point scale ranging from "not at all" to "very much". The selected items were slightly rephrased to be in the first person. Following these revisions, the final items were: (1) "I am concerned that information about me could be found on an old computer." (2) "I am concerned that my e-mails are being read by other people." The response scale ranged from (1) hardly ever to (5) almost always. Privacy concern was computed as the average of the items ($r = .493$, $p < .001$, MN = 2.11, SD = 1.00), with a range from 1 to 5, higher scores indicating greater privacy concern.

2.4.4 *Use of mobile device to connect to wireless and social networks*

A selection of questions from [30] were utilized in order to learn more about the behaviors of our participants and their past experience. We first wanted to find out how often (but not why) our participants connected to public wireless: "How frequently do you connect your devices (work iPad, tablet, and laptop) to a public wireless network with your mobile phone?" The response options ranged from (a) "daily," (b) "weekly," (c) "monthly," (d) "less than one a month," to (e) "never." Participants' responses were grouped into two groups (daily vs. other) in subsequent analyses due to small cell sizes <20 (responses available for 96 participants). Participants fell into two different groups: those who used public wireless to connect via mobile devices at least once a month ($n = 42$) and those who never connected to public wireless ($n = 54$).

Participants were also asked about their use of social networks using the following statement: "How likely are you to use your mobile devices to access social networking sites (e.g., Facebook, Twitter, MySpace, Instagrams, LinkedIn, YouTube, etc.)?" The response options were identical for both questions: (1) daily, (2) weekly, (3) monthly, (4) less than once a month, and (5) never. Responses were available for 95 participants. These were grouped into three groups. Those who accessed social networking sites daily ($n = 27$), those who accessed it weekly to at least once monthly ($n = 25$), and those who never accessed social networks via their mobile devices ($n = 43$). Finally, the survey asked participants whether or not they had already experienced negative consequences due to their online

activity. The question was "Have you ever experienced any negative consequences from your online activities?" and had five possible response options: (1) "No, I have not experienced any negative experiences." (2) "Yes, my account information has been stolen." (3) "Yes, my credit card information has been stolen." (4) "Yes, my personal information has been compromised." (5) "Yes, other" (to be completed by participant). Participant responses (98 responses available) were put into two groups in subsequent analyses due to small cell sizes. One group represented the group who reported no negative experience ($n = 68$). The second group included participants with different types of negative experiences ($n = 30$), including those who had their account detail or credit cards stolen, their personal information compromised or reported some other incident.

2.4.5 Control variables

Control variables included participant age, gender, their use of computers outside of the university, their self-reported IT proficiency and technological device ownership. IT proficiency varied between novice ($n = 21$), intermediate ($n = 71$) and professional ($n = 8$). Participants were also requested to report how many devices they owned (from a list of seven options, including options such as a computer, tablet, and removable media such as iPod or flash drive, mobile phone with 3G, mobile phone without 3G, Bluetooth equipment, and Internet enabled games). On average, our participants owned four such devices (MN = 3.83, SD = 1.05, range 2–7).

3 Results

3.1 Descriptive results

Impulsivity correlated weakly and marginally significantly with privacy attitudes ($r = .187$, $p = .058$) but significantly and negatively with age ($r = -.265$, $p = .008$, $n = 98$). It is well known that impulsivity decreases with age. The observed correlation is therefore in line with previous research but also points to the need to control for age in subsequent analyses. Finally, greater use of technology via multiple devices was positively correlated with increased privacy concerns ($r = .212$, $p = .034$).

Hypothesis 1 Impulsivity is a negative predictor of the number of features processed.

The extent to which impulsivity is related to attentional processing was examined using eye-tracking data as indicated by the number of pre-defined areas of interest (AOI, the features of interest) processed on each screen—described here as an *attention score*. This analysis involved eye-tracking data that were obtained for 40 of the 104 participants. This number was limited due to the effort required to evaluate all recordings individually for each of the 40 participants (resulting in 40*5 individual recordings).

In addition to the impulsivity and attention scores, the analysis included the effective data capture reports (effectiveness percentage provided by the software for each participant, representing the number of valid gaze points) as a control variable into the model. Regression analysis suggests a good model fit ($R^2 = .293$, $R^2_{adj} = .254$, $F(2,36) = 7.472$, $p = .002$). The regression coefficient indicates that as impulsivity increases, attention decreases, that is, the number of AOIs (=features) reviewed by participants declined ($b = -2.448$, $\beta = -.334$, $t = -2.380$, $p = .023$). The results support hypothesis 1.

The scatter plot and slope illustrates the relationship between the number of features processed and impulsivity (Fig. 1). Features included symbols such as padlocks, strength indicators and the names of various options. Higher impulsivity is associated with lower number of features processed. The eye-tracking group ($n = 40$) did not differ significantly from the non-eye-tracked group ($n = 64$) in terms of their level of impulsivity or the decisions participants made (network options selected). As a result, these statistics are not reported here.

In further analysis, we also assessed if feature processing in the eye-tracking may have been influenced by previous use of Wi-Fi networks. However, no significant group differences were observed in terms of how participants used public wireless services. This suggests that previous experience and use of open wireless do not explain our findings (e.g., no support was obtained for the suggestion that more impulsive candidates may have been

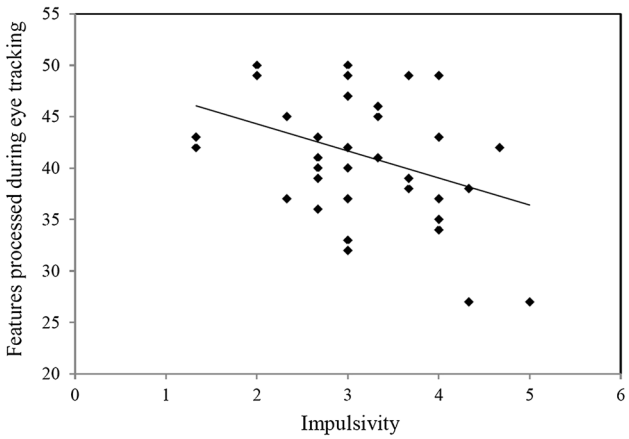

Fig. 1 Relationship between impulsiveness and number of features processed

less experienced and thus reviewed the Android screens more haphazardly).

Hypothesis 2 Impulsivity is negatively correlated with privacy concern.

As privacy attitude is known to be associated with age and device ownership, we controlled for these in our regression analysis [$R^2 = .083$, $R^2_{adj} = .054$, $F(3,94) = 2.845$, $p = .042$]. The regression coefficient suggests that impulsivity was positively associated with privacy concern, not negatively as we had predicted ($b = .279$, $\beta = .218$, $t = 2.130$, $p = .036$).

This result was surprising and clearly does not support our hypothesis that privacy concern would be lower in more impulsive individuals. Several explanations exist. It is possible that experience with security-related incidents could play a role (i.e. more impulsive individuals may have experienced more adverse events in the past). The survey provided us with some information about our participants' past experience with security-related incidents. This therefore enabled us to conduct an exploratory ANCOVA to examine a potential link between impulsiveness and security experience, controlling for age once more (gender was not a significant covariate). The results were not significant [$F(1,95) = .712$, $p = .401$]. Impulsivity was not significantly different between users who had no negative experiences to report (MN = 3.23, SD = .80, $n = 68$) and those who had reported negative experiences in the past (MN = 3.30, SD = .80, $n = 30$). Past experience of security-related incidents between more and less impulsive users did not appear to be the driving force behind greater privacy concerns voiced by the more impulsive users. Another explanation—not verifiable within our current dataset—is that more impulsive individuals are aware that their behavior may leave them vulnerable to risk and are accordingly more anxious about the corresponding privacy threat.

Hypothesis 3 Impulsivity is positively correlated with mobile device use and social media access.

Some work suggests that when individuals use social media to check e-mail and connect with others, they are also more likely to suffer negative spillover effects on both work and home life [4]. More impulsive individuals may be even more likely to engage in such behaviors on the spur of the moment. We therefore tested whether more impulsive individuals would also be more likely to connect to wireless networks via their mobile devices (data were available for 96 out of 104 participants due to eight missing values). The impulsivity score of the group that never used public wireless ($n = 54$) was examined in relation to the group that used mobile devices at least once a month to connect online ($n = 42$). This was assessed using ANCOVA controlling for age, as device ownership and use may be dependent on age via income and employment status. A significant group difference emerged [$F(1,93) = 9.374$, $p = .003$]. Those who never used public wireless with the help of their mobile devices also had significantly lower impulsivity (MN = 3.05, SD = .84) compared to those participants who used their mobile devices to do so at least once a month in order to check their e-mails (MN = 3.50, SD = .67). This indicates that those who were more driven to connect to public wireless to check e-mails also tended to be more impulsive.

Another question was whether or not impulsivity was associated with more frequent accessing of social networks via their mobile devices (iPad, tablet and laptop). A significant group difference was observed when conducting ANCOVA, again controlling for age [$F(2,91) = 6.100$, $p = .003$]. Individuals who never access social networks via their mobile devices were significantly less impulsive (MN = 2.97, SD = .87, $n = 43$) compared to individuals who accessed social networks daily ($p = .012$; MN = 3.44, SD = .76, $n = 27$) and those who accessed such networks at least weekly to monthly on their mobile devices ($p = .017$; MN = 3.48, SD = .58, $n = 25$). These results provide some support for hypothesis 3. More impulsive users had used their mobile devices to connect to public wireless more frequently than less impulsive users. This also extended to the frequency with which they would then access social network via public networks.

4 Discussion

Impulsivity and mobile device use may have an important impact on work–life balance and security decisions. Previous work had suggested an important role for personality in security-related decision-making, influencing the effectiveness of security messages [35], vulnerability to phishing [27], perceptions of risk [55] and attitudes related to information security [63]. This study aimed to add to our current understanding of the role of impulsivity in security-related behaviors around wireless network selection and mobile phone use.

Our design and hypotheses were based on existing evidence around poorer self-regulation, distractibility and lower deliberation associated with higher impulsiveness [28, 32, 58]. All of these aspects may also affect how and what type of security-related decisions individuals may make when switching back and forth between tasks and when switching between home and work contexts. Behaviors of interest included selecting less secure wireless network options, less attentive visual processing of information, the regular use of wireless public networks and the frequency with which individuals connect to

(potentially insecure) social networks using their mobile devices. In addition, the omnipresence of the mobile phone and the culture of connecting "anytime, anywhere" may negatively impact temporal and geographical boundaries that separate work and home [see 49].

We first examined the type of decisions our users tended to make in a selection task. Using eye-tracking data, we found that those with higher impulsivity processed fewer details when making decisions. This suggests that impulsive individuals did not attend to all pieces of information available to them [18]. This is not so much a concern when the best options come first in a menu list. But it can be a problem when better decision-making relies on a longer search of all menu options or a more considered weighing up of alternatives. These findings are therefore in line with the cited evidence above that impulsiveness is associated with problems of attention and deliberation [58] which we have now shown to lead to poor security decisions.

Based on previous evidence, we expected more impulsive individuals to show reduced privacy concern. However, the association between impulsivity and privacy concerns was positive, i.e., more impulsive individuals reported greater, not less, concern. This suggests that more impulsive individuals may be more casual about security settings, but nonetheless feel concern about the kinds of information they share (as indicated by the self-reported privacy concern). This result was not influenced by whether or not participants had experienced more negative events in the past. It is possible that impulsive individuals do not deliberate on their options at the time, or indeed that they exhibit a certain behavioral rigidity that means they find it difficult to change or alter choices [22], but they may be aware that these choices leave them vulnerable and this awareness feeds into a greater concern for privacy. Finally, our finding that more impulsive individuals made more regular use of public networks and were more frequent users of social media—activities that expose individuals to potential security and privacy risks—may be related again to the kinds of poorer self-regulation reported for more impulsive individuals [5].

In conclusion, the results of our study showed that impulsive people are more likely to make use of their mobiles to connect to social media and that they are also less likely to engage in careful deliberation before connecting to wireless networks. This means that impulsive individuals are more likely to place both personal and work data at risk, given the rise of BYOD working and the increased use of the mobile phone to complete and respond to both home and work activities. We already know that boundary management between home and work is difficult [23], but our findings suggest that personality may also play a role here—impulsive people may find it harder to manage those boundaries and may risk data security breaches as a consequence. However, it is important to note that we used a student sample in this study. While many students struggle to combine their academic and working lives, they nonetheless enjoy a degree of flexibility that is unusual for those in full time employment and that may limit the extent to which of our findings can be generalized to other contexts.

4.1 Practical implications for the use of mobile technologies and work–life balance

The findings have some practical implications for work-related decision-making, particularly for impulsive individuals faced with various challenges when trying to manage their work–life balance. Impulsive decision-making may be functional in many specific settings [18], especially when the decision is routine and the decision-maker is an expert who is able to assess the situation based on very few cues. However, in these situations more impulsive individuals may not be fully aware or cognizant of all possible (including negative) outcomes of their behaviors [44], which then results in suboptimal decisions and errors. This has implications not only for the work–life balance of more impulsive workers, but also for the ways in which mobile working might be supported, both by policy [59] and by design [17], while also reducing associated data risks, health and home life. Some research has already shown that employees have greater difficulties managing the boundaries between work and life when they are also in the habit of continuously accessing work-related e-mails and cannot tear themselves away from work, even when in the home [25]. The current study's findings suggest that these tendencies may be even more exacerbated when employees are more impulsive, thus potentially threatening their ability to manage work–life boundaries even more. We outline the practical implications and potential starting points next.

One suggestion, based on our work, would be to consider more carefully just how personality and risk are related and how this may inform design (e.g. we might wish to explore design interventions that might encourage more deliberation). Past research has suggested that campaigns to raise security awareness may be more effective if it were possible to consider the personality profile of the recipients [35] and identify those who are more likely to engage in more risky decisions in the area of information security [57]. In terms of work–life balance, it is important that organizations and human resource managers recognize and potentially limit the very pervasive and negative impact of work-related communication in employees' personal lives [66], particularly in virtual work settings [52]. The negative impact may be even more pronounced when personal and work lives overlap, which is often the

case when employees use social networks that include colleagues as well as friends. This has led some organizations to provide guidelines to their employees on how they should use social media as they recognize that their employees will be in touch with both colleagues and friends.

Another suggestion is to find ways to address individual sensitivity to undesirable outcomes and emphasize the potential benefits of certain behaviors. This could be particularly helpful for impulsive individuals who also appear to have low sensitivity to negative consequences in online contexts [44]. These circumstances may not only apply to their decisions online, but may also affect their ability to balance time dedicated to personal or work-related tasks and interactions [25]. This may also lead to problems due to cloud computing and online monitoring [15]. Design interventions could heighten an individual's sense of anticipated regret about making a potentially disadvantageous decision. Past work has shown that greater anticipated regret can sway individuals to choose safer options, in the presence of both potential gains and losses [70]. So one strategy would be to increase perceived regret about making poor decisions. Another strategy could be to remove unnecessary time constraints as these may reduce the pressure on an individual and could lead to more deliberation when problem solving [47]. A related option is to emphasize the security benefits, especially when this may require some effort [67]. Increasing the personal relevance of consequences and making intangible benefits more explicit for the mobile worker (e.g., in terms of safety gains) may increase sensitivity of potential effects as most people have only abstract notions of information security [67].

A related suggestion would be to consider the timing and design of computer-mediated instructions and system warnings that could increase adherence and responsiveness of users, especially those who are more likely to make impulsive decisions to get online at all times during the day. This could be achieved by "timing-out" important messages and preventing users from clicking away messages within a specific period (too short for them to have read and process the information). In this paper, we have reported that impulsivity results in fewer features being processed on a screen featuring different choices. Indicators of security risks need to be particularly salient. For instance, color coding and order of wireless options (by security levels) have been shown to positively influence security decisions, even for those with higher levels of impulsivity [10]. More inexperienced (such as students) and impulsive individuals may also benefit from reminders about time spent on tasks in different contexts, for instance, how much time spent on social media during the work day, or work e-mail outside of the work day and learning about how to better manage their time [68] and work–life demands [40].

4.2 Future research

Future research may wish to examine a number of areas. We first consider the security-specific concerns, before addressing issues around maintaining or supporting a work–life balance. These focus on domain-specific impulsivity research, the utility of including other measures to assess the relationship between impulsiveness and attention and the potential influence of other individual differences (such as self-efficacy).

Our first suggestion concerns the breadth of impulsiveness as a construct. Different types of impulsiveness are reported in the literature, and these may carry different implications for security behaviors. For example, making decisions quickly is representative of *cognitive impulsiveness*, while acting without careful thought is often associated with *motor impulsivity*. The lack of planning or forethought in activities has been described as *non-planning impulsiveness* (see more information in [2]). In our study, we were particularly interested in non-planning and attentional impulsivity as pertinent to online activities as these may be assessed more readily using self-report using the Diminished Impulse Scale and eye tracking. However, other measures may also be available to assess these subcomponents of impulsiveness. A variety of other measures for impulsivity exists such as the Impulsivity Inventory [18]; Impulsiveness Scale [21] and; the impulse subscale of the Adolescent Decision-Making Questionnaire [62]. These measures also tap different behavioral components of impulsivity (see discussion in [22]). More research in this area could provide more insight—it would be particularly interesting to see work that explores the role of domain-specific impulsivity and how this relates to more or less effective boundary management as well as (sub)optimal security-related decision-making.

The second suggestion concerns the way interaction design may compensate for impulsivity (using notifications and display options). Our broader work is focused on the role of design in influencing choice and has currently investigated interface and message interventions around network choice, cookie acceptance, error reporting and phish detection. However, this sits along other research within the area of usable security and HCI which has identified design elements to nudge other security behaviors, e.g., improve password strength [64]. This is only the tip of the iceberg with regards to the kinds of security behaviors that people are expected to show at work. More work is needed in this area not only to address ways to improve security decisions and behaviors, but also to reduce the dependency on the users for the overall security of the system.

The current literature says relatively little about the context for security interactions. Despite the recognition

that BYOD is both a growing trend and a security threat, very few studies have considered the interplay between the context for work and home interactions and the security implications of eroding the work–life barrier. We do know that smartphone users often experience greater work–home interference because they find it difficult to disengage and actively recover from work-related stresses [16]. This stress may not only affect how well work and life demands are managed, but also compromise security-related decision-making by affecting attention and deliberation of options. Further evidence to date suggests that workaholism tends to predict compulsive Internet use [51], which demonstrates how problematic the persistent and continuous use of communication technologies may become for balancing the demands of work and home life. Future research might explore the ways in which impulsive individuals self-regulate their behavior, so as to understand more precisely how they come to establish and maintain the barriers between home and work (as well the effect of distractors such as notifications and similar on maintaining boundaries).

And finally, the interaction between work and task demands, personality and interface or work design have not been fully explored. More work is needed to understand how personality relates to mobile working. Future work might explore other personality characteristics such as self-efficacy [33], conscientiousness or the role and impact of distraction (from the Online Cognition Scale). The distraction subscale in this measure might able to give some insight into how individuals use the Internet to prevaricate and reduce stress [13] and how this links to their use of BYOD technology, online networks, and their management of conflict and work-life boundaries.

Acknowledgments This research is supported by Engineering and Physical Sciences Research Council (EPSRC) Grant EP/K006568 Choice Architecture for Information Security, part of the Government Communications Headquarters (GCHQ)/EPSRC Research Institute in Science of Cyber Security, UK. We gratefully acknowledge the support and the contribution of Kerry Rulton and Minh Tran as well as our colleagues James Turland, Iryna Yevseyevna and Aad van Moorsel from the School of Computing Science at Newcastle University.

References

1. Almuhimedi H, Schaub F, Sadeh N, Adjerid I, Acquisti A, Gluck J, Cranor L, Agarwal Y (2015) Your location has been shared 5398 times!: a field study on mobile app privacy nudging. In: Proceedings of the 33rd annual ACM conference on human factors in computing systems (pp 787–796). ACM
2. Barratt ES (1985) Impulsiveness subtraits: arousal and information processing. In: Spence JT, Izard CE (eds) Motivation, emotion, and personality. Elsevier, North Holland, pp 137–146
3. Beautement A, Sasse MA, Wonham M (2008) The compliance budget: managing security behaviour in organisations. In: New security paradigms: proceedings of the 2008 workshop (NSPW), pp 47–58. doi:10.1145/1595676.1595684
4. Berkowsky RW (2013) When you just cannot get away. Inform Commun Soc 16(4):519–541. doi:10.1080/1369118X.2013.772650
5. Billieux J, Van Der Linden M (2012) Problematic use of the internet and self-regulation: a review of the initial studies. Open Addict J 5(1:M4):24–29. doi:10.2174/1874941001205010024
6. Bittman JE, Brown JE, Wajcman J (2009) The mobile phone, perpetual contact and time pressure. Work Employ Soc 23:673–691. doi:10.1177/0950017009344910
7. Buchanan T, Paine C, Joinson AN, Reips U-R (2007) Development of measures of online privacy concern and protection for use on the Internet. J Assoc Inf Sci Technol 58(2):157–165. doi:10.1002/asi.20459
8. Chin E, Porter Felt A, Sekar V, Wagner D (2012) Measuring user confidence in smartphone security and privacy. In: Proceedings of the eighth symposium on usable privacy and security (SOUPS '12). ACM, New York, NY, USA
9. Cousins K, Robey D (2015) Managing work-life boundaries with mobile technologies: an interpretive study of mobile work practices. Inform Tech People 28(1):34–71
10. Coventry L, Jeske D, Briggs P (2014) Perceptions and actions: combining privacy and risk perceptions to better understand user behavior. In: Workshop proposal, symposium on usable privacy and security (SOUPS) 2014, July 9–11, 2014, Menlo Park, CA
11. Darley WK, Blankson C, Luethge DJ (2010) Toward an integrated framework for online consumer behavior and decision making process: a review. Psychol Mark 27(2):94–116. doi:10.1002/mar.20322
12. Darwish A, Bataineh E (2012) Eye tracking analysis of browser security indicators. Proc Comput Syst Ind Inform ICCSII 1(6):18–20. doi:10.1109/ICCSII.2012.6454330
13. Davis RA, Flett GL, Besser A (2002) Validation of a new scale for measuring problematic Internet use: implications for pre-employment screening. Cyber Psychol Behav 5(4):331–345. doi:10.1089/109493102760275581
14. De Luca A, Lindqvist J (2015) Is Secure and usable smartphone authentication asking too much? Computer 48(5):64–68
15. De Oliveira AS, Sendor J, Garaga A, Jenatton K (2013) Monitoring personal data transfers in the cloud.cloud computing technology and science (CloudCom). IEEE 5th international conference on, vol 1, pp 347–354, 2–5 December 2013. doi:10.1109/CloudCom.2013.52
16. Derks D, ten Brummelhuis LL, Zecic D, Bakker AB (2012) Switching on and off …: does smartphone use obstruct the possibility to engage in recovery activities? Eur J Work Org Psychol 23:80–90. doi:10.1080/1359432X.2012.711013
17. Derks D, van Mierlo H, Schmitz EB (2014) A diary study on work-related smartphone use, psychological detachment and exhaustion: examining the role of the perceived segmentation norm. J Occup Health Psy 19(1):74–84. doi:10.1037/a0035076
18. Dickman SJ (1990) Functional and dysfunctional impulsivity: personality and cognitive correlates. J Pers Soc Psychol 58:95–102. doi:10.1037/0022-3514.58.1.95
19. Duxbury L, Higgins C, Smart R, Stevenson M (2014) Mobile technology and boundary permeability. Br J Manag 25:570–588. doi:10.1111/1467-8551.12027

20. Ebeling-Witte S, Frank ML, Lester D (2007) Shyness, internet use, and personality. Cyberpsychol Behav 10(5):713–716. doi:10.1089/cpb.2007.9964
21. Eysenck SBG, Pearson PR, Easting G, Allsopp JF (1985) Age norms for impulsiveness, venturesomeness and empathy in adults. Pers Individ Differ 6:613–619. doi:10.1016/0191-8869(85)90011-X
22. Franken IHA, van Strien JW, Nijs I, Muris P (2008) Impulsivity is associated with behavioral decision-making deficits. Psychiatry Res 158:155–163. doi:10.1016/j.psychres.2007.06.002
23. Frampton BD, Child JT (2013) Friend or not to friend: co-worker Facebook friend requests as an application of communication privacy management theory. Comput Hum Behav 29:2257–2264. doi:10.1016/j.chb.2013.05.006
24. Furnell S, Rajendran A (2012) Understanding the influences on information security behaviour. Comput Fraud Sec. doi:10.1016/S1361-3723(12)70053-2
25. Grant C, Wallace LM, Spurgeon PC (2013) An exploration of the psychological factors affecting remote e-worker's job effectiveness, well-being and work-life balance. Empl Relat 35(5):527–546. doi:10.1108/ER-08-2012-0059
26. Günay E (2012) The effects of Internet use on individual's socialization based on personality traits. New Yeni Symp J 50(3):123–133
27. Halevi T, Lewis J, Memon N (2013) A pilot study of cyber security and privacy related behavior and personality traits. In: International worldwide web conference, May 13–17; Rio de Janeiro, Brazil
28. Halpern DF (1989) Thought and knowledge: an introduction to critical thinking, 2nd edn. Erlbaum Publishing, Hillsdale
29. Hu Q, Xu Z, Dinev T, Ling H (2011) Does deterrence work in reducing information security policy abuse by employees? Commun ACM 54(6):54–60. doi:10.1145/1953122.1953142
30. IFIP (2013) IFIP Technical Committee 11, Working Group 12: human aspects of information security and assurance, global information security awareness survey. http://www.ifip11-12.org/index.php/page/take-survey
31. Jia R (2012) Computer playfulness, internet dependency and their relationships with online activity types and student academic performance. J Behav Addict 1(2):74. doi:10.1556/JBA.1.2012.2.5
32. Johnson-Laird PN (1988) A taxonomy of thinking. In: Sternberg RJ, Smith EE (eds) The psychology of human thought. Cambridge University Press, Cambridge, pp 429–457
33. Johnston AC, Warkentin M (2010) Fear appeals and information security behaviors: an empirical study. MIS Q 34(3):549–566
34. Kahneman D (2011) Thinking, fast and slow. Farrar, Straus and Giroux, New York
35. Kajzer M, D'Arcy J, Crowell CR, Striegel A, van Bruggen D (2014) An exploratory investigation of message-person congruence in information security awareness campaigns. Comput Secur 43:64–76. doi:10.1016/j.cose.2014.03.003
36. Katz FH (2005) The effect of a university information security survey on instructing methods in information security. In: Proceedings of the second annual conference on information security curriculum development, pp 43–48. doi:10.1145/1107622.1107633
37. Kritzinger E, von Solms SH (2010) Cyber security for home users: a new way of protection through awareness enforcement. Comput Secur 29:840–847. doi:10.1016/j.cose.2010.08.001
38. Leclercq-Vandelannoitte A, Isaac H, Kalika M (2014) Mobile information systems and organisational control: beyond the panopticon metaphor? Eur J Inform Syst 23:543–557. doi:10.1057/ejis.2014.11
39. Lee HW, Choi JS, Shin YC, Lee JY, Jung HY, Kwon JS (2012) Impulsivity in internet addiction: a comparison with pathological gambling. Cyberpsychol Behav Soc Netw 15:373–377. doi:10.1089/cyber.2012.0063
40. Lowe J, Gayle V (2007) Exploring the work/life/study balance: the experience of higher education students in a Scottish further education college. J Further Higher Educ 31(3):225–238. doi:10.1080/03098770701424942
41. Luna L (2011) Smart-device woes. Urgent Commun 29(8):8
42. Magid V, Colder CR (2007) The UPPS impulsive behavior scale: factor structure and associations with college drinking. Pers Individ Differ 43:1927–1937. doi:10.1016/j.paid.2007.06.013
43. Marshall NL, Barnett RC (1993) Work-family strains and gains among two-earner couples. J Community Psychol 21:64–78. doi:10.1002/1520-6629(199301)21:1<64:AID-JCOP2290210108>3.0.CO;2-P
44. Martin LE, Potts GF (2009) Impulsivity in decision-making: an event-related potential investigation. Pers Individ Differ 46:303–308. doi:10.1016/j.paid.2008.10.019
45. Mason, G. (2010). Part-time higher education students in the UK: Statistical Review. Revised report to Higher Education Careers Services Unit (HECSU) for Birkbeck/NIESR Project on Career decision-making and career development of HE students. http://www.hecsu.ac.uk/assets/assets/documents/Part-time_HE_students_in_the_UK_Statistical_Review_April_2010.pdf
46. Muslukhov I, Boshmaf Y, Kuo C, Lester J, Beznosov K (2013) Know your enemy: the risk of unauthorized access in smartphones by insiders. In: Proceedings of the 15th international conference on human–computer interaction with mobile devices and services (MobileHCI '13). ACM, New York, NY, USA, pp 271–280. doi:10.1145/2493190.2493223
47. Ordóñez L, Benson L III (1997) Decisions under time pressure: how time constraint affects risky decision making. Organ Behav Hum Decis 71(2):121–140. doi:10.1006/obhd.1997.2717
48. Özcan NK, Buzlu S (2007) Internet use and its relation with the psychosocial situation for a sample of university students. Cyber Psychol Behav 10(6):767–772. doi:10.1089/cpb.2007.9953
49. Prasopoulou E, Pouloudi A, Panteli N (2006) Enacting new temporal boundaries: the role of mobile phones. Eur J Inform Syst 13:277–284. doi:10.1057/palgrave.ejis.3000617
50. Price K, Kirwan G (2013) Personality caught in the social net: facebook phishing. In: Power A, Kirwan G (eds) Cyberpsychology and new media: a thematic reader. Psychology Press, Abingdon, pp 126–135
51. Quiñones-García C, Korak-Kakabadse N (2014) Compulsive internet use in adults: a study of prevalence and drivers within the current economic climate in the UK. Comput Hum Behav 30:171–180. doi:10.1016/j.chb.2013.08.004
52. Rafnsdóttir GL, Stefánsson AS (2014) Virtual work and work-life balance for managers. Int J Bus Manage 9:1–12. doi:10.5539/ijbm.v9n11p1
53. Rashid F (2012) Turning mobile devices into university dorm keys. eWeek 29(3):18–19
54. Rezgui Y, Marks A (2008) Information security awareness in higher education: an exploratory study. Comput Secur 27:241–253. doi:10.1016/j.cose.2008.07.008
55. Riquelme IP, Roman S (2014) Is the influence of privacy and security on online trust the same for all type of consumers? Electron Mark 24(2):135–149. doi:10.1007/s12525-013-0145-3
56. Russello G, Conti M, Crispo B, Fernandes E (2012) MOSES: supporting operation modes on smartphones. In: Proceedings of the 17th ACM symposium on access control models and technologies (SACMAT '12). ACM, New York, NY, USA, pp 3–12. doi:10.1145/2295136.2295140
57. Shropshire J, Warkentin M, Johnston A, Schmidt M (2006) Personality and IT security: an application of the five-factor model. In: Proceedings of the twelfth Americas conference on information systems, Acapulco, Mexico, August 4–6

58. Stanford MS, Mathias CW, Dougherty DM, Lake SL, Anderson NE, Patton JH (2009) Fifty years of the Barratt Impulsiveness Scale: an update and review. Pers Individ Differ 47:385–395. doi:10.1016/j.paid.2009.04.008
59. Tarafdar M, Darcy J, Turel O, Gupta A (2015) The dark side of information technology. MIT Sloan Manage Rev 56:61–70. doi:10.1111/isj.12015
60. Thaler RH, Sunstein CR (2008) Nudge. Improving decisions about health, wealth and happiness. Penguin, London
61. Turland J, Coventry L, Jeske D, Briggs P, van Moorsel A (2015) Nudging towards security: Developing an application for wireless network selection for android phones. In: Proceedings of the 2015 British HCI Conference, pp 193–201. ACM
62. Tuinstra J, van Sonderen FLP, Groothoff JW, van den Heuvel WJA, Post D (2000) Reliability, validity and structure of the adolescent decision making questionnaire among adolescents in The Netherlands. Pers Individ Differ 28:273–285. doi:10.1016/S0191-8869(99)00096-3
63. Uffen J, Guhr N, Breitner MH (2012) Personality traits and information security management: An empirical study of information security executives. In: Proceedings of thirty third international conference on information systems (ICIS), Orlando, USA
64. Ur B, Kelley PG, Komanduri S, Lee J, Maass M, Mazurek ML, Cranor LF (2012). How does your password measure up? The effect of strength meters on password creation. In: Proceedings of USENIX security symposium, pp 65–80
65. Wajcman J, Bittman M, Brown JE (2008) Families without borders: mobile phones, connectedness and work-home divisions. Sociol 42(4):635–652. doi:10.1177/0038038508091620
66. Waller AD, Ragsdell G (2012) The impact of e-mail on work-life balance. Aslib Proceedings 64:154–177. doi:10.1108/00012531211215178
67. West R (2008) The psychology of security. Commun ACM 51(3):34–40
68. Wittmann M, Paulus MP (2008) Decision making, impulsivity and time perception. Trends Cogn Sci 12(1):7–12. doi:10.1016/j.tics.2007.10.004
69. Wright KB, Abendschein B, Wombacher K, O'Connor M, Hoffman M, Dempsey M, Krull C, Dewes A, Shelton A (2014) Work-related communication technology use outside of regular work hours and work life conflict: the influence of communication technologies on perceived work life conflict, burnout, job satisfaction, and turnover intention. Manage Commun Q 28:507–530. doi:10.1177/0893318914533332
70. Zeelenberg M, Beattie J, van der Pligt J, de Vries NK (1996) Consequences of regret aversion: effects of expected feedback on risky decision making. Organ Behav Hum Decis 65(2):148–158. doi:10.1006/obhd.1996.0013