

Unfolding the Popularity of Video Conferencing Apps – A Privacy Calculus Perspective

Abstract

Videoconferencing (VC) applications (apps) have surged in popularity as an alternative to face-to-face communications especially during the COVID-19 pandemic. Although VC apps offer myriad benefits, it has caught much media attention owing to concerns of privacy infringements. This study examines the key determinants of working professional's intentions to use VC apps in the backdrop of this conflicting duality. A conceptual research model is proposed that is based on theoretical foundations of privacy calculus and extended with conceptualizations of mobile users' information privacy concerns (MUIPC), trust, technicality, ubiquity, as well as theoretical underpinnings of social presence theory. Structural equation modelling (SEM) is used to empirically test the model using data collected from 487 working professionals. For researchers, the study offers insights on the extent to which social richness and technological capabilities afforded by the virtual environment serve as predictors of the continuance intentions of using VC apps. Researchers may also find the model applicable to other studies of surveillance-based technologies. For practitioners, key recommendations pivotal to the design and development mobile videoconferencing apps are presented to ensure higher acceptance and continued usage of VC apps in professional settings.

Keywords: video conferencing apps, privacy calculus, mobile users' information privacy concerns, social richness.

1 Introduction

The COVID-19 pandemic outbreak with its travel restrictions, social distancing, and shelter in place measures, has dramatically influenced the way individuals communicate and collaborate (Adom et al., 2020; Hakim et al., 2020; Kagan et al., 2020; Kumar & Kulkarni, 2020). Video conferencing (VC) applications (apps) have gained in popularity as a result of the need for social distancing and remote work (Billingsley, 2020). The recent growth in the number of VC app users has been unprecedented (Kagan et al., 2020). Professionals in healthcare, education, business, government, and other sectors have embraced VC apps at substantive rate to cope with the COVID-19 pandemic crisis (Patnaik, 2020). VC apps have aided employees to continue operations and meet contractual commitments with limited interruptions (Adom et al., 2020; Hakim et al., 2020; Kumar & Kulkarni, 2020). While VC apps provide a convenient way for peers to communicate and collaborate, it also creates a channel for severe privacy violations that range from theft of personal and financial information to loss of intellectual property, productivity, and reputation (Ahmad, 2020). For instance, incidents of Zoom bombing raised grave privacy concerns as uninvited attendees joined VC meeting purely by guessing meeting IDs (Billingsley, 2020). Violations in the VC environment enable intruders gain access to sensitive data (Kagan et al., 2020) and place both professionals as well as organizations at the risk (Neustaedter et al., 2018). Furthermore, concerns of VC app companies collecting data without informing users, routing meeting encryption keys through servers located in adversary countries (Brewster, 2020), sharing personal information with third parties without

consent (Adom et al., 2020; Brewster, 2020), and making misleading claims of end-to-end encryption (Brewster, 2020) have only increased during the recent pandemic.

Despite the privacy risks and concerns, the use of VC apps have surged and the professionals' dependence on VC platforms have increased (Aiken, 2020). To put in context, as of December 2019, approximately 10 million daily meetings were conducted on Zoom, and as of March 2020, the number of daily Zoom users increased to 200 million and the daily Microsoft Teams users escalated to 1.56 million (Patnaik, 2020).

Literature refer the above behavior as a *privacy paradox*, where, contrary to concerns of privacy infringements, individuals are willing to disclose personal information, as long as they get something in return (Kokolakis, 2017). Individuals engage in a risk-benefit evaluation referred to as the *privacy calculus* of information disclosure (Dinev & Hart, 2006). The outcome of such an evaluation is *perceived value*, which, when positive, favors personal information disclosure and continued usage of technology and, when negative, signals reluctance towards information disclosure and use of technology (Morosan & DeFranco, 2015; Shaw & Sergueeva, 2019; Wiegard & Breitner, 2019; Xu et al., 2011). For our study, we argue that professionals make trade-off decisions to determine whether the risks of privacy violations are worth the benefits of using VC apps. The question remains as to what trade-offs professionals are willing to make in the face of information privacy concerns associated with VC apps.

While there is a plethora of research on VC, most have treated VC as part of collaborative technologies or social media technologies (see Table 1 in Appendix for a review of related literature). To the best of our knowledge, scholarship has not examined the dual paths of perceived benefits and risks on the perceived value of VC apps at the individual level. Furthermore, no studies have conducted an in-depth empirical assessment of how the unique characteristics of VC apps contribute to its popularity and continued use despite the associated privacy risks. In this research, we seek to unfold the privacy paradox of VC apps based on the theoretical foundations of privacy calculus. The research thus targeted two related objectives. First, it aims to assess the attitude of professionals in the calculus of decisions to use VC apps. Second, the study seeks to investigate the extent to which social richness and technological capabilities afforded by the virtual environment serve as predictors of the professionals' continuance intentions of using VC apps. To address the first study objective, we developed a conceptual research model rooted in the theoretical foundations of privacy calculus (Culnan & Armstrong, 1999; Dinev & Hart, 2006). To gain a deeper understanding of how the salient features of the medium influence the continuing use of VC apps, we extended the model to include the conceptualization of mobile users' information privacy concerns (Belanger & Crossler, 2019; Xu et al., 2012), trust (Chrysochoidis et al., 2009), technicality (Kim et al., 2007), ubiquity (Okazaki & Mendez, 2013), and theoretical underpinnings of social presence theory (Short

et al., 1976). Thus, the conceptual research model meaningfully and comprehensively integrates the technological and social constructs at play when using VC apps.

The study makes three notable contributions. First, the study enhances our understanding of the individual attitude and behavior towards VC app usage in the professional context. It sheds light on the utility of the dual path privacy calculus model to scrutinize new and emergent technologies that reshape the workplace. Second, the research builds on prior scholarship in areas such as privacy calculus, MUIPC, ubiquity, and social presence that are crucial to online collaborative technologies. The research thus contributes to the continuum of knowledge that parallels the progression of contemporary technologies as they move through stages of inflated expectation to the plateau of productivity (Linden & Fenn, 2003). Third, the conceptual research model that we tested enabled us to assess social richness and technological capabilities of VC apps framed in the dichotomy of associated information privacy concerns and recognized benefits. The study thus leads to a better understanding of how professional engage with VC apps. The findings have implications for the development of privacy sensitive mobile VC apps that suit the needs of the new age mobile workers. Thus, the study is not only timely and appropriate to the pandemic context, but also relevant and topical as the surge in popularity and use of VC apps is likely to be a sustained workplace norm.

The rest of this paper is organized as follows. Section 2 provides an overview of VC apps and theoretical foundations of the study. The conceptual model and related hypotheses are presented in section 3. Section 4 discusses the research methodology and design, followed by the analysis of results in section 5. In section 6, we discuss the main findings of the study, along with the theoretical contributions and practical implications. Finally, we conclude the paper by discussing the limitations of the study and avenues for future research.

2 Theoretical background

2.1 Video conferencing applications

Video conferencing is an interactive platform that facilitates communication and collaboration between two or more individuals in real time through a combination of high-quality audio and video over internet protocol (IP) network (Billingsley, 2020). Various mobile VC apps such as Skype, Zoom, Google Hangout, Zoho Meeting, Eyeson, Cisco Webex, GoToMeeting, and Signal exist in market (Gray et al., 2020). VC apps enable individuals to interact from any location, even while in transit, using data capable mobile devices such as smart phones, tablets, and laptops over cellular or Wi-fi network (Zhang et al., 2016). Modern VC apps incorporate a variety of sophisticated features including screen sharing, recording, chat, document sharing, polling, whiteboard, and breakout rooms, thereby facilitating greater engagement

and interactivity. As a ubiquitous communication technology (Zhang et al., 2016), VC apps enable professionals to meaningfully maintain and sustain social presence in the virtual world (Brown et al., 2010; Short et al., 1976) along with the added benefits of convenience, ease of use, cost savings (Archibald et al., 2019), time savings, and spatial flexibility (Li et al., 2020).

Nevertheless, VC apps have been consistently subjected to criticisms over security concerns and privacy violations. They range from unencrypted communications for unpaid users to vulnerabilities that enable malware execution on participants' devices (Kagan et al., 2020). Under these circumstances, a better understanding of what drives professionals to continue using VC apps become crucial to ensure a virtual environment that preserves security and privacy of participating professionals.

Prior literature has mostly considered VC as a part of collaborative technologies (Brown et al., 2010) or a social media technologies (Gruzd et al., 2012; Sarwar et al., 2019). Related research have investigated their role in knowledge sharing (Pillet & Carillo, 2016), research practices (Gruzd et al., 2012), behavioral intentions (Brown et al., 2010; Liu & Alexander, 2017; Maican et al., 2019), and enhancement of collaborative learning and learner performance (Sarwar et al., 2019). To the best of our knowledge, none of the studies have exclusively studied the adoption or intentions to use consumer grade VC apps. In addition, none of the studies investigated the influence of privacy concerns on the individual's adoption or intentions to use VC apps. Table 1 in Appendix provides a summary of the studies on VC apps, including the theoretical models, methods, and the context of each.

2.2 Privacy calculus theory

The concept of calculus was introduced by Laufer and Wolfe (1977), where the authors argue that an individual's decision to disclose personal information depends on three critical aspects of behavior calculus: institutional norms of appropriate behavior, expected benefits, and unpredictable consequences. Following the assumption that the personal information disclosure can be thought of as tradeable good, Culnan and Armstrong (1999) argued that individuals' decision to disclose personal information involved a subjective cost benefit analysis, whereby individuals are willing to disclose personal information in exchange of social and economic benefits, provided the personal information is used fairly. Dinev and Hart (2006) extended the work of Culnan and Armstrong (1999) in the context of the Internet, and noted that the individual's decision to disclose personal information is influenced by a set of beliefs that are contrary in nature. The influence of one belief may outweigh the other to the extent that the resulting stronger belief influences the individual's behavioral intentions such as disclosure of the personal information (Dinev & Hart, 2006). They further argue that personal information disclosure introduces considerable uncertainties about who has the access to the information and how it is used. The uncertainties are balanced by the individual's perceptions of various factors such as trust in the organization (Malhotra et al., 2004), benefits of

information disclosure, functional congruence and perceived informativeness (Li et al., 2016), perceived enjoyment, ease of use (Wiegard & Breitner, 2019), and perceived usefulness (Shaw & Sergueeva, 2019; Wiegard & Breitner, 2019). When engaging in privacy calculus, consumers do not treat privacy as an absolute societal value, but rather as a commodity characterized by economic value (Smith et al., 2011).

Theoretical foundations of privacy calculus have been used in various contexts including location based mobile devices (Xu et al., 2009), location aware marketing (Xu et al., 2011), social networking systems (Krasnova et al., 2012), e-commerce (Li et al., 2010), location based social network services (Zhao et al., 2012), mobile applications (Keith et al., 2016; Wang et al., 2016); adoption behaviors associated with wearable devices (Li et al., 2016), personalized nutrition services (Berezowska et al., 2015), mobile applications (Pentina et al., 2016), loyalty intentions in hotel booking (Ozturk et al., 2017) and Pay-As-You-Live (PAYL) services (Wiegard & Breitner, 2019). In this study, we use privacy calculus to examine individuals' intentions to use VC apps in a professional context.

2.3 Mobile users' information privacy concerns (MUIPC)

Privacy concerns is one of the most commonly studied constructs in the empirical literature (Belanger & Crossler, 2019). Related research has mainly investigated two key conceptualizations: concerns for information privacy (CFIP) proposed by Smith et al. (1996) and the Internet user's information privacy concerns (IUIPC) proposed by Malhotra et al. (2004). CFIP was developed to measure individuals' concerns around organizational information privacy practices, whereas IUIPC was proposed to measure Internet user's information privacy concerns. Building upon these conceptualizations and drawing on communication privacy management theory, Xu et al. (2012) proposed mobile users' information privacy concerns (MUIPC) to measure users' privacy concerns in the context of mobile environment.

Due to aggressive practices of data collection and sharing employed by applications running on mobile devices, privacy concerns of mobile users are likely to be different from online users (Xu et al., 2012). Enhanced capabilities of mobile devices such as sensors, cameras, microphone, GPS, and accelerometer enable mobile applications to profile and target specific individuals. Mobile apps have the potential to record extremely sensitive and private information such as contacts, photos, videos, daily conversations, and location information. Such powerful eavesdropping capabilities aptly raise significant privacy concerns (Mirzamohammadi & Sani, 2018). MUIPC is thus considered a suitable and valid instrument to investigate privacy concerns of users in the mobile environment (Degirmenci, 2020). Regardless of the context, it is important to note that prior literature has considered privacy concerns as a predictor of both perceived privacy risks and trust (Kehr et al., 2015; Malhotra et al., 2004; Van Slyke et al., 2006; Wu et al., 2015).

MUIPC entails three dimensions: perceived surveillance, perceived intrusion, and secondary use of personal information. Perceived surveillance is the mobile users' concern regarding personal information watched, listened or recorded. Perceived intrusion relates to mobile users' concern of mobile apps possessing or soliciting users' personal information, and creating discomfort, interruption, and harm through unwanted presence. Secondary use of personal information relates to concerns about vendors using personal information for secondary purposes or revealing it to unauthorized entities without consent or awareness of the mobile app user (Xu et al., 2012)

We use MUIPC as the instrument of our study because our main interest is VC apps, and our focus is on professionals utilizing the platform for virtual collaboration and communication.

2.4 Social presence

The concept of social presence was introduced in the seminal work by Short et al. (1976). They define social presence as the “the degree of salience of the other person in the interaction and the consequent salience of the interpersonal relationships...” (p. 65). Short et al. (1976) hypothesized social presence as not just the quality of media itself, but also as a perceptual and attitudinal dimension of individuals in the mediated communication. Communication media vary in their degree of social presence. Different factors such as, the capacity to transmit facial expression, posture, direction of looking, dress, and non-verbal cues contribute to the social presence of a medium. Short et al. (1976) argues face-to-face communication to be highest in social presence, followed by video communication, audio, and written memos. They note that it is the individuals who determine how different factors contribute towards social presence of a communication medium.

In a review of prior studies, Biocca (2003) identified four key themes where social presence is measured: perceived social richness of the medium, involvement, immediacy or intimacy, social judgement of others, and sense of being together. Of the four themes, Biocca (2003) noted that perceived social richness of the medium was the most widely used construct. As per this construct, users do not assess their experience of others, but indirectly assess the effect of the medium, i.e., the social and emotional capabilities of the communication medium (Biocca, 2003). In this study we use perceived social richness of the medium, since one of our research objectives was to determine how professionals assess the social and emotional capabilities afforded by VC apps.

2.5 Ubiquity

Ubiquity is one of the most important characteristics of mobile devices and services. Initial discussion of ubiquity in published literature was in early 2000s in the context of U-commerce (Watson et al., 2002), wireless advertising (Barnes, 2002), and mobile commerce (Balasubraman et al., 2002). Since then, ubiquity has been conceptualized in a variety of ways.

Building on the work of Watson et al. (2002), Junglas and Watson (2006) proposed ubiquity as one of the four *u-commerce* constructs comprising reachability, accessibility and portability. Junglas and Watson (2006) defined ubiquity as “the drive to have access to information unconstrained by time and space” (p.578). The authors noted that in the ubiquitous world, individuals are capable of accessing the network at any time (reachability and accessibility) from anywhere (portability), and in turn, reachable at anytime and anywhere. Kim and Garrison (2009) conceptualized ubiquity as “individual’s perception regarding the extent to which mobile wireless technology (MWT) provides personalized and uninterrupted connection and communications between the individual and other individuals and/or networks” (p.326).

Based on the review of literature, Okazaki et al. (2012) conceptualized ubiquity as “the interconnectedness dimension of time savings and spatial flexibility” (p. 172). Time savings represents the mental calculation that a user performs of the time saved when performing activities using a mobile service. Spatial flexibility represents the perceived mobility that a mobile service provides to a user to perform the activities without being restricted at one place (Okazaki et al., 2012). Okazaki and Mendez (2013) developed and tested a formal measurement instrument for perceived ubiquity of mobile services. Perceived ubiquity was proposed as a second-order construct with four first-order factors: continuity, immediacy, portability, and searchability. Continuity relates to the state or aspect of being continuous i.e., the unique ability of mobile technology to provide continuous access to services that cannot be offered by traditional channels. Immediacy relates to one’s perceived amount of time between an action and its resulting outcomes (i.e., quickness of an action or occurrence). Portability is the quality of being light enough to be carried anywhere. And, searchability refers to information or data search in computer mediated environments and the capability to make thorough examinations (Okazaki & Mendez, 2013).

3 Conceptual model and hypotheses

To unfold the impact on user’s continuance intentions regarding VC apps use, we developed a conceptual research model. The model combines MUIPC (Belanger & Crossler, 2019; Xu et al., 2012), social presence (Short et al., 1976), and ubiquity (Okazaki & Mendez, 2013; Okazaki et al., 2012) with privacy calculus theory (Culnan & Armstrong, 1999; Dinev & Hart, 2006) as shown in Figure 1. MUIPC is a second order formative construct (Xu et al., 2012) based on perceived surveillance, perceived intrusion, and secondary use of personal information. Ubiquity is the other second order formative construct. In our study, we assess ubiquity based on five first order reflective constructs specified in the prior literature: time savings, spatial flexibility, portability, immediacy, and continuity. Since video conferencing is not used to search data and information, searchability was not included in our study. The second order constructs are represented by the double-bordered boxes as shown in Figure 1.

As discussed previously, trust and social presence are two other constructs that influence privacy calculus, which in itself is an assessment of the effects of perceived risks and benefits on perceived value. Technicality is considered to moderate the continuance intentions of using VC apps. The conceptual research model thus consolidates constructs from prior theories that are relevant to assess the perceived value of VC apps and the individual's continuing intentions of using VC apps.

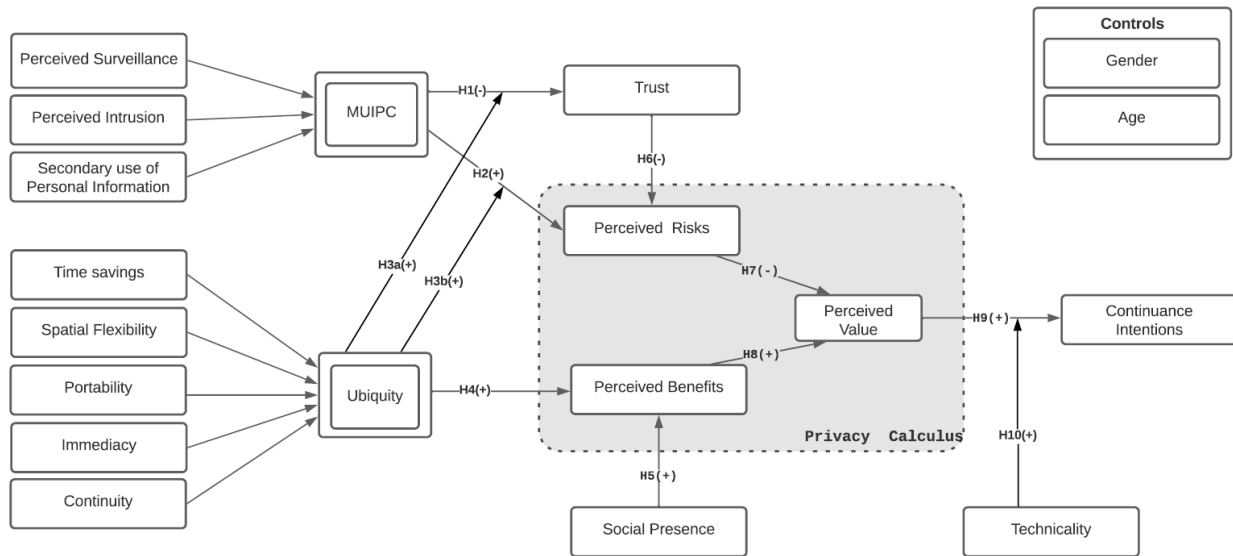


Figure 1. Conceptual research model.

3.1 The role of information privacy concerns

Information privacy concerns reflect the apprehension of professionals regarding opportunistic behaviors around information collection, use, and handling. Although the highly interactive nature of VC platforms offer indisputable advantages (Venkatesh et al., 2009), surveillance capabilities of VC apps (Yuan et al., 2016), software implementation flaws or even deliberate backdoors allow others (Clarke, 2017) to monitor or record users' activities. Users of VC apps are concerned of vendors revealing, sharing and misusing information without their awareness or approval (Aiken, 2020). A recent example is that of Zoom, a popular VC app, collecting and selling data to Facebook without explicit consent of the user (Hamilton, 2020). Communications using VC apps can result in privacy invasion as it reveals information about the user's appearances, place and behavioral context (Neustaedter et al., 2015; O'Hara et al., 2009). To some extent, privacy concerns of VC apps and its impacts on trust and perceived risks parallel to those of Internet and Online users (Bansal et al., 2016; Malhotra et al., 2004). Consistent with the prior literature, a higher degree of concern regarding information privacy is therefore likely to be associated with lower trust in VC apps and increased perceptions of risks associated with its use. Thus, we hypothesize

H1. *Mobile Users' Information Privacy Concerns (MUIPC) have a negative effect on Trust.*

H2. Mobile Users' Information Privacy Concerns (MUIPC) have a positive effect on Perceived Risks.

3.2 The role of ubiquity

In this study, we conceptualize ubiquity as the degree to which professionals believe that VC apps provide uninterrupted connection and access to peers anytime and anywhere (Arpaci, 2016). When working together, professionals often engage in discussions, negotiations, instant feedback, and decision making. These tasks require frequent back and forth transmission of small quantities of information among the parties (Straub & Karahanna, 1998). Individuals chose collaboration technologies based on their ability to reach their peers, i.e., whether the collaborating partner is immediately available for communication or not (Straub & Karahanna, 1998). VC apps provide professionals an “always available link” to effectively, efficiently, and instantly connect with colleagues irrespective of spatial distances (Brown et al., 2010). The spatial flexibility results in time and cost savings, convenience, and ease of use (Armfield et al., 2015), which in turn positively influences professionals’ perceptions of VC apps as being beneficial.

Past studies have found that ubiquity also moderates the influence of information privacy concerns on trust and perceived risks (Okazaki et al., 2009). This moderating effect similarly applies to the context of VC apps. For instance, mobile devices enable professionals to gain continuous access to VC services even while they are on the move (Wang et al., 2016). While professionals may find the continuity feature beneficial, the vendors also have the ability to collect rich information about customers relative to their location. The increased anxiety arising from ubiquitous monitoring and tracking is likely to intensify the role of information privacy concerns on perceived risks and trust, i.e., the more ubiquitous the VC platform, the stronger the effect of MUIPC on perceived risks and trust. Hence, we hypothesize

H3a. Ubiquity positively moderates the effect of MUIPC on Trust.

H3b. Ubiquity positively moderates the effect of MUIPC on Perceived Risks.

H4. Ubiquity has a positive effect on Perceived Benefits.

3.3 The role of social presence

Social presence is the degree to which professionals perceive interactions with their peers over VC apps as sociable, warm, personal, and humanizing. A media that allow for communication of maximum number of audio and visual cues such as gestures or facial expressions would lead to higher degree of social presence (Rogers & Lea, 2005), ensure quality in the outcomes (Yoo & Alavi, 2001), and effectiveness in completing work related tasks (Brown et al., 2010). Social presence on communication media is suited for ambiguous and equivocal tasks that require group consensus, and resolution of differences in opinions and

viewpoints among individuals (Yoo & Alavi, 2001). Elevated social presence fosters cognitive and affective reactions in the individuals that range from perceived usefulness and ease of use (Hew et al., 2018) to enhanced performance and usefulness (Brown et al., 2010). VC apps enable social presence as it emulates face-to-face interactions by conveying a variety of social cues such as audio, video, and emoticons. Therefore, we hypothesize

H5. Social Presence has a positive effect on Perceived Benefits.

3.4 The role of trust

Trust represents the users' confidence in the reliability and trustworthiness in VC app with regards to protecting and safe handling of personal information. Individuals' trust functions differently according to how a specific risk is communicated or managed. The perception of risk is a consequence of trust, rather than a determinant of trust, in that if individuals' trust the organization to manage specific risks, they perceive the risk to be smaller and the benefits to be higher (Chrysochoidis et al., 2009). The professionals' trust in VC apps depends upon privacy and security of information access and protection models deployed by the service providers. If service providers follow strict security and privacy policies, then trust is enhanced, which in turn lower perceived risks associated with use of VC apps. Thus, we hypothesize

H6. Trust has a negative effect on Perceived Risks.

3.5 The role of privacy calculus

Perceived benefits represent favorable net of outcomes or compensations resulting from the disclosure of personal information (Smith et al., 2011). On the contrary, perceived privacy risks represent the degree to which individuals think there is a high potential for loss associated with the disclosure of personal information (Malhotra et al., 2004). In using VC apps, professionals perform a risk benefit analysis (privacy calculus) to account for the value gained from its use and the risks to information privacy. Although a personal weighting calculus (Zeithaml, 1988) of this nature may be conducted by professionals (i.e., assessing the cumulative effect of risks and benefits), prior literature suggests that users are likely to give up a certain degree of privacy in exchange for benefits (Shaw & Sergueeva, 2019; Wiegard & Breitner, 2019; Xu et al., 2011).

VC apps offer unique advantages to professionals' in terms of ease of use and effectiveness in completing work-related tasks. Thus, a higher assessment of the benefits of VC apps would lead to higher perceived value from its use. Conversely, perceived privacy risk negatively influences perceptions of value (Shaw & Sergueeva, 2019; Wiegard & Breitner, 2019; Xu et al., 2011). In today's environment, mobile apps not only collect personal information explicitly, but they also covertly capture information such as location, conversations, credit card information, timestamped messages, and activity history (Shaw & Sergueeva, 2019). This is also true of VC apps as was recently revealed

in the high-profile examples of Zoom and Facebook (Koch, 2020). Incidents such as these increase vulnerabilities and intrusions into one's life, and the likely assessment of higher perceived risks of using VC apps. Hence

H7. *Perceived Risks have a negative effect on Perceived Value.*

H8. *Perceived Benefits have a positive effect on Perceived Value.*

3.6 The role of perceived value

Perceived value is the overall assessment of utility of a product based on perceptions of what is received and what is given (Zeithaml, 1988). It is the overall estimation of the choice object and once that overall estimation is internalized, it becomes a criterion for a consumer's choice behavior (Kim et al., 2007; Xu et al., 2009) such as adoption intentions (Kim et al., 2007), use intentions (Shaw & Sergueeva, 2019), and willingness to share personal information with service vendors (Xu et al., 2009).

Until recently, extant literature had excluded perceived value as an explicit latent variable in privacy calculus models. Newer studies (Morosan & DeFranco, 2015; Shaw & Sergueeva, 2019; Xu et al., 2011) argue that perceived value represents a natural evaluative artefact that aggregates the risk benefit assessment process, and thus its inclusion is essential to complete the privacy calculus model. Following the conceptualization of Zeithaml (1988), we refer to perceived value of VC apps as the professionals' overall perception of the value of VC apps based on benefits obtained and sacrifices made to use it. Furthermore, we hypothesize that higher utilitarian value derived from using VC apps motivates professionals to continue using video-conferencing apps. Hence

H9. *Perceived value positively influences the continuance intentions to use VC apps.*

3.7 The role of technicality

Following the conceptualization of Kim et al. (2007), we define technicality of video-conferencing as the degree to which professionals perceive VC apps to be technically excellent in the terms of ease of use, reliability, connectivity, and efficiency. Ease of use is the overall user-friendliness of the system, i.e., the degree to which professionals perceive VC apps to be free of physical and mental effort. Reliability denotes that the system is free from errors and is consistently available and secure. Connectivity signifies that the connection is instant and straightforward. Efficiency signifies quick loading or response time (Kim et al., 2007).

Technical difficulties experienced while using a technology hinder the user from realizing its full benefits, and consequently requiring the investment of cognitive effort to use the technology (Setterstrom et al., 2013). Technical difficulties cause psychological discomfort including anxiety and

fear, frustration, annoyance, and mental fatigue (Kim et al., 2007). Technicality is a significant predictor of an individuals' perceptions of value of a technology, regardless of whether the adoption pertains to initial usage or continuance usage (Setterstrom et al., 2013). In our study, we assess the moderating effects of technicality on the relationship between perceived value and continuing intentions to use VC apps. We posit that perceived value leading to continuance intentions is susceptible to change with the level of technicality experienced in VC apps usage. Specifically, technicality negatively moderates the influence of perceived value on continuance intentions. As the physical and mental effort required to use VC apps increases, intentions to continue using VC apps decrease. Thus

H10. Technicality negatively moderates the effect of Perceived Value on Continuance Intentions.

Finally, similar to other studies, we treat gender and age as control variables (Kordzadeh & Warren, 2017; Wu et al., 2014).

4 Research methodology

4.1 Measurement

To test the theoretical constructs, a survey instrument was developed based on constructs and items from published literature on MUIPC, trust, social presence, ubiquity, and privacy calculus (see Table 2 in Appendix). The items were measured on a seven-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree). Age was measured in years and gender was represented using a dummy variable where 0 represented women. The study was reviewed and approved by the ethics board prior to starting data collection.

4.2 Data collection

The survey instrument was shared on LinkedIn professional social media network, and via its direct messaging feature. A two-step approach was taken to collect data using the questionnaire. First, the “key informant” data collection approach (Pinsonneault & Kraemer, 1993) was performed. This was essential in order to identify fitting respondents to whom direct messages were sent on LinkedIn during Fall 2020. All respondents were given the option of receiving the results of this study. This translated to a total of 2471 LinkedIn users that were contacted. Second, follow-up messages were sent to the users who did not provide feedback or confirmed that the survey would be answered and submitted. 487 completed and valid responses were received at the end of eight weeks, corresponding to a 19.7% response rate. The Kolmogorov–Smirnov (K–S) test indicated that non-response bias was not present (Ryans, 1974) between early and late respondents. Common method bias was evaluated using two approaches. The first approach was the Harman’s one-factor test (Podsakoff et al., 2003).

The second approach was using the marker viable approach (Lindell & Whitney, 2001), with the addition of a theoretically irrelevant marker variable in the model, retrieving a low value (Johnson et al., 2011) of 0.023 (2.3%) as the maximum shared variance with other variables. Both approaches indicated no significant common method bias in the data. The demographic characteristics of the sample is shown in Table 3 of the Appendix.

5 Data analysis

Partial least squares (PLS) technique was utilized for the analysis of data. PLS technique is used for a variety of reasons. First, PLS analysis enables the use of formative indicators to model latent constructs (Goo et al., 2009). Second, this technique mitigates restrictive distributional assumptions being significantly different from zero (Fornell & Bookstein, 1982; Gefen & Straub, 2005; Goode et al., 2015). Third, it is helpful to analyze models that have not been tested before (Ke et al., 2009; Teo et al., 2003). Since our conceptual model includes formative constructs, variables that are not normally distributed ($p < 0.01$, Kolmogorov–Smirnov's test), and has never been tested before, PLS technique is an applicable and suitable technique for our study (Chin et al., 2003).

5.1 Measurement model

A measurement model was developed to assess construct reliability, convergent validity, discriminatory validity, and indicator reliability. The measurement model results are shown in Tables 4, 5, and 6 of the Appendix. Table 4 shows descriptive statistics, composite reliability (CR), correlation, and average variance extracted (AVE), whereas Table 5 shows loadings and cross loadings. Table 6 in Appendix shows heterotrait-monotrait (HTMT) ratio.

Composite reliability (CR) was used to test construct reliability. All constructs have CR higher than 0.7 indicating the suitability and internal consistency of the constructs (Henseler et al., 2009; Straub, 1989). Average variance extracted (AVE) was used to test convergent validity. All constructs have AVE higher than 0.50 signifying convergent validity of the measurement model (Fornell & Larcker, 1981; Hair et al., 2012). To achieve indicator reliability, the loading should be higher than 0.7 (Churchill Jr, 1979; Henseler et al., 2009). Two items (PS1 and C3) were therefore removed due to low factor loading. All other loadings are higher than 0.7, thus validating indicator reliability.

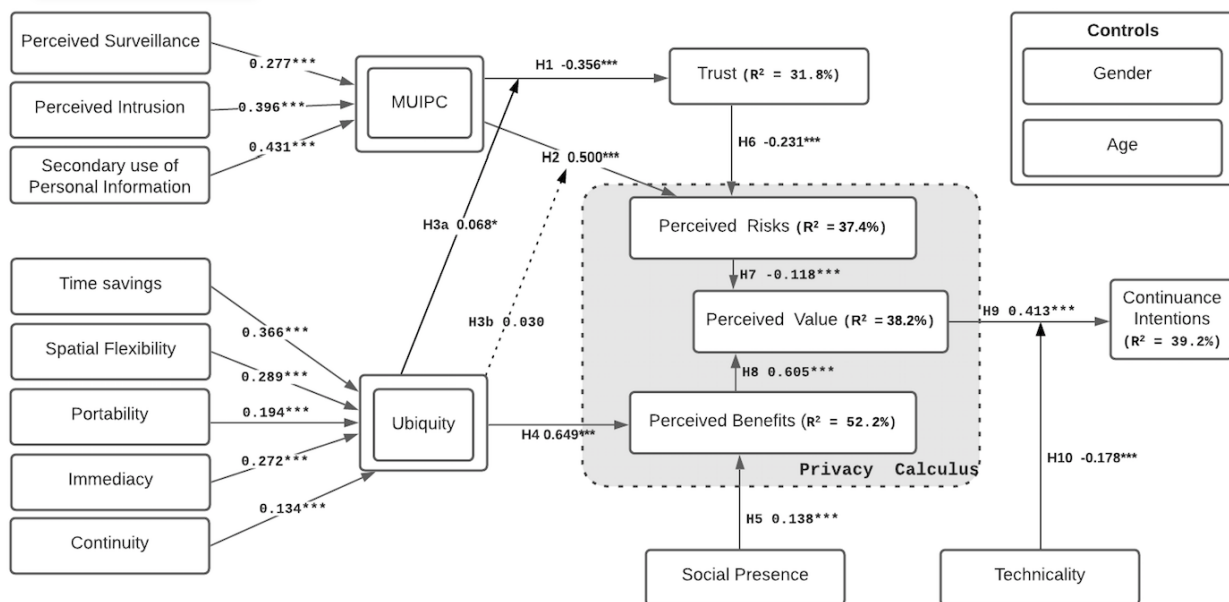
Fornell-Larcker criterion, loadings, and HTMT were used to assess discriminant validity of the constructs (Henseler et al., 2015). Fornell-Larcker criterion requires that square root of AVE should be higher than correlation between constructs (Chin, 1998), and satisfied by the measurement model. The second criterion that the loadings (in bold) should be greater than cross-loadings is also satisfied (Chin, 1998). Additionally, all HTMT values are lower than the threshold of 0.9 providing further

confirmation of the discriminant validity of the constructs. The constructs and the conceptual research model are thus appropriate to test the structural model.

The measurement model was used to analyze the significance, weights, and multicollinearity of constructs. Variance inflation factor (VIF) statistic was used to assess multicollinearity (see Table 7 in Appendix), which ranged between 1.461 and 2.871. Multicollinearity among the variables is not an issue in the measurement model since VIF values are below the threshold of 3.3 (Lee & Xia, 2010). Furthermore, all weights are statistically significant, and therefore we can conclude that the structural model also presents good measurement model.

5.2 Test of the structural model

The structural model (Figure 2) presents the PLS results including variation explained and the path coefficients. The significance levels of the hypothesized construct were performed using bootstrapping with 5000 resamples. All constructs present VIF lower than 1.467, thus implying that the model does not present multicollinearity (Hair Jr et al., 2016).



(Note: *** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$).

Figure 2. Structural model

The model explains 31.8% of variation in trust, confirms the negative effect of MUIPC ($\beta = -0.356$; $p < 0.01$), and the moderating effect of ubiquity ($\beta = 0.068$; $p < 0.10$) on trust. Consequently, H1 and H3a are supported.

The model explains 37.4% of the variation in perceived risks. Trust ($\beta = -0.231$; $p < 0.01$), alongside MUIPC ($\beta = 0.500$; $p < 0.01$) are statistically significant in explaining perceived risks of VC apps. However,

the moderating role of ubiquity on the relation between MUIPC and perceived risks was not found to be significant. Therefore, H2 and H6 are supported, whereas H3b is not supported.

With regard to perceived value, the model explains 38.2% of its variation. Perceived risks ($\beta = -0.118$; $p < 0.01$) and perceived benefits ($\beta = 0.605$; $p < 0.01$) are found to be statistically significant in explaining perceived value of VC apps. Thus, H7 and H8 are supported.

The model also explains 52.2% of the variation in perceived benefits. The positive effect of ubiquity ($\beta = 0.649$; $p < 0.01$) and social presence ($\beta = 0.138$; $p < 0.01$) on the benefits of VC apps are statistically significant, thus supporting H4 and H5.

Finally, the model explains 39.2% of the variation in continuance intentions. The positive influence of perceived value ($\beta = 0.413$; $p < 0.01$), and the negative moderating effect of technicality ($\beta = -0.178$; $p < 0.01$) are also supported, thus confirming H9 and H10.

6 Discussion

The objective of this study was to investigate and understand the attitude of working professionals to continue using VC apps despite the privacy risks associated with its use.

The findings from our study indicate that information privacy concerns positively influence perceived risks associated with the use of VC apps. A closer look at the survey results suggest that professionals are more concerned about secondary use of personal information and privacy intrusion when compared to surveillance potential of VC apps. Although professionals may find VC apps effective for collaboration and sharing of work-related information, the platform also offers other entities (e.g., app vendors and peers) direct and indirect access to personal information. Secondary use of personal information concerns the use of information available via VC apps without authorization. The study confirms that professionals are concerned their private information might be more readily available to others than they are willing or comfortable to share.

A related finding confirmed by the study is the mediating role of trust in the relationship between information privacy concerns and the perceived risks of VC apps. The results indicate that information privacy concerns impact trust, which in turn influences perceived risks. Perception of risk as a consequent of trust has been suggested in the past (Chrysochoidis et al., 2009). The triadic construct relationships confirmed by our study indicates that the perception of risk involved in using a VC app is lower when professionals have more trust in the information privacy policies of the app vendor.

With regards to ubiquity, the study found that professionals value the benefits of portability and spatial flexibility provided by VC apps. It enabled them to quickly reach and communicate with peers from any place and wherever they go. Professionals felt that VC apps provided an effective way

to manage time and make life easier by enabling flexibility in schedule. They did not feel that VC apps compromised social presence. The likely explanation is that the capability to mirror natural face-to-face communications through the use of both audio and video enable VC apps to produce perceptions of human closeness and warmth. The study findings also indicated that technicality negatively moderated the relationship between perceived value and continuance intentions to use VC apps. This implies that, when professionals perceive VC apps to take longer time to connect, respond, or use, their perceptions of value decrease and subsequently their intentions of continued use.

Ubiquity also moderated the relationship between MUIPC and trust, but its moderating effect on the relationship between MUIPC and perceived risks was found to be insignificant. One possible explanation is the strength of relationship between the respective constructs. As noted by Okazaki et al. (2009), the magnitude of impact of the moderator depends on the relationship that it is set to modify. The stronger the relationship between the constructs, the less influence the moderator has on the relationship (Okazaki et al., 2009). Our study suggests that MUIPC has a stronger relationship to perceived risks compared to its relationship with trust. Our analysis enabled us to understand the relationships even further. For instance, MUIPC is more important in explaining trust in the environment with high ubiquity, i.e., the higher moderating effect of ubiquity influences the negative relation between MUIPC and trust as seen in Figure 3a.

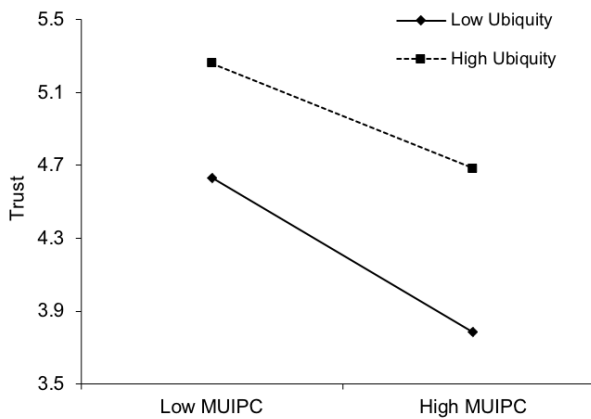


Fig. 3a. Moderation effect of ubiquity in MUIPC on Trust

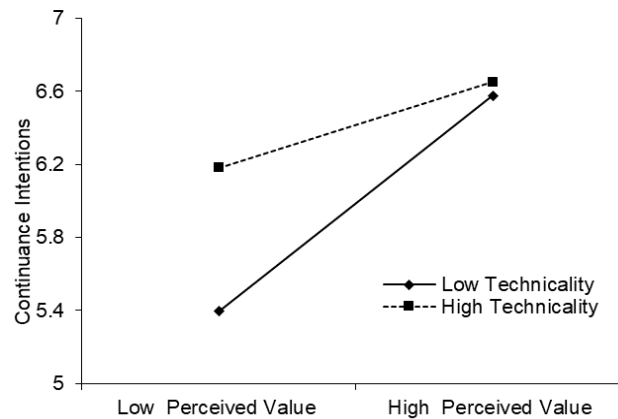


Fig. 3b. Moderation effect of technicality in perceived value on continuance intentions

The study found the negative relationship between perceived risks and perceived value, and the positive relationship between perceived benefits and perceived value to be significant. These findings suggest that professionals recognize the benefits of time savings, spatial flexibility, portability, immediacy, continuity, and social richness provided by VC apps. However, the benefits are tempered by privacy risks of VC apps such as the potential for surveillance and sharing of information by unauthorized entities without

consent. Nevertheless, when perceived benefits and perceived risks are evaluated in tandem, it appears that professionals' perception of value is more strongly influenced by the benefits offered by VC apps than associated risks, resulting in the positive evaluation of its perceived value. In sum, the study highlights the subsistence of privacy paradox in the use of VC app, wherein professionals overcome concerns of privacy risks when the perceived benefits are higher. The professionals chose to use VC apps despite the risks associated with its usage. This finding draws parallel to prior studies related to location aware mobile apps (Morosan & DeFranco, 2015; Wang et al., 2016; Xu et al., 2011).

The findings also indicated the positive influence of perceived value on intentions to continue using VC apps. This suggests that perceived value shapes the professionals continuing intentions to use VC apps. The findings are consistent with past studies of mobile services (Shaw & Sergueeva, 2019; Wang et al., 2020) in that users continue to engage in mobile services as long it has a value for them. Additionally, perceived value is more important to explain continuance intentions in the environments where VC app have low technicality, i.e., when technicality is high the perceived value is not as important in explaining continuance intentions, as can be seen in Figure 3b.

6.1 Theoretical contribution

The research makes three significant theoretical contributions. First, the main objective of the study was to examine the attitude and behavior of professionals towards VC apps and its continuing use. To do so, the study proposed and evaluated a conceptual research model that combined the dual path model of privacy calculus theory with social and technological constructs representing information privacy concerns, technicality, ubiquity, and social presence. The model can be applied in other studies of surveillance-based technologies (e.g., electronic IDs, facial recognition, and smart badges) that are similarly veiled in the dichotomy of established benefits and legitimate privacy concerns.

Second, this research extends prior work on privacy calculus (Dinev & Hart, 2006) by identifying four underlying factors that influence the dual paths of perceived benefits and risks leading to the perceived value of VC apps. The study thus addresses the call by Xu et al. (2009) to investigate how users of surveillance prone technologies balance the tradeoffs between privacy risks and benefits. Our study found that ubiquity and social presence enhance professionals' perception of the benefits, whereas MUIPC and trust influence perceptions of risks. Additionally, by modeling ubiquity and MUIPC as second-order formative constructs our study offers further depth in analysis and understanding of their significance in the popularity of VC apps. In doing so, our study addresses the call by Xu et al. (2012) for additional research that contributes to the generalizability of MUIPC across differing mobile applications and environments.

Finally, to the best of our knowledge, no study has investigated the combined effect of technology constructs and social constructs on the continuing use of VC apps. Our study found that technicality moderated the perceived value of VC app and continuance intentions. In contrast, prior studies (Kim et al., 2007) regarded technicality as an antecedent of perceived value. Our study thus opens new avenues of for investigating the moderating effects of other dimensions of technicality such as connectivity, ease of use, service reliability, and response time. It further highlights the incremental knowledge building based on published literature as discussed in the next section.

6.2 Practical Implications

The study offers notable insights as to why professionals are willing to risk privacy infringements in exchange for the benefits of VC platforms. As prospects of remote work and virtual collaboration becomes the new workforce norm, professionals will continue to engage in a dynamic adjustment process in which potential privacy risks are weighed against the rewards of using VC apps. The question then is, what would ensure that privacy calculus of individuals favor VC app platforms and the subsequent willingness to continue its use. The findings of our study suggest that VC app vendors and policy makers could play a role in reducing the risk perceptions of professionals who regularly engage with VC apps.

In our comprehensive review of the literature, we found few recent studies that have made notable recommendations for the constructs we analyzed in our research model. For example, to improve ubiquity, Zhou (2012) proposed a technological focus on backend systems that provide reliable and immediate access to services, and Archibald et al. (2019) recommended continuous cycle of improvements to services to enhance performance and functionalities. Similarly, Park and Sundar (2015) recommended the use of presence establishing strategies to improve synchronicity. Ye et al. (2020) and Park and Sundar (2015) suggested the use of humanizing cues to increase social presence on virtual platforms. Published literature recommends explicitly stated privacy policies (Wiegard & Breitner, 2019; Xu et al., 2008), procedural fairness in information practices (Culnan & Armstrong, 1999), vendor transparency regarding personal data collection, storage, and use (Plangger & Montecchi, 2020), trusted app model where vendors work with trusted third party entities to certify privacy practices (Ozturk et al., 2017), and the use of privacy discrepancy interface that allow personalization of privacy levels (Jackson & Wang, 2018) to lower privacy risks of VC apps. The summary of recommendations is shown in Table 1. When reviewed in the milieu of our empirical analysis, the recommendations would be meaningful for VC app vendors to enhance their products and services.

Table 1. Recommendations for VC app vendors to enhance perceived value of VC apps

Study constructs	Prior studies that have addressed the constructs	Recommendations
------------------	--	-----------------

Ubiquity	(Archibald et al., 2019; Zhou, 2012)	Technological improvements to backend systems to enhance reliability, immediacy, continuity, and portability.
Social presence	(Park & Sundar, 2015)	Improve synchronicity
Privacy risks	(Ye et al., 2020)	Humanizing cues
	(Culnan & Armstrong, 1999; Lin et al., 2012; Wiegard & Breitner, 2019; Zhou, 2011)	Procedural fairness in information practices Explicitly stated privacy policies
	(Lin et al., 2012; Plangger & Montecchi, 2020; Xu et al., 2008)	Vendor assurance and transparency of personal information protection
	(Jackson & Wang, 2018; Ozturk et al., 2017)	Trusted app model with privacy seal; privacy discrepancy interface

The findings of our study also benefit policy makers such as the United States Federal Communications Commission (FCC) and the European Commission for Communications, who regulate communications over radio, TV, satellite, and cable Internet. Policies that mandate the inclusion of information privacy check and balances would ensure that confidentiality and security of information are maintained in modern collaborative platforms. Comprehensive policies and guidelines focused on safeguarding privacy concerns would warrant a secure environment for all employees to participate virtually regardless of the nature of workplace.

7 Conclusion

This study aimed to improve our understanding of individual attitude and behavior of professionals towards VC apps usage despite the stark contradiction between its recognized benefits and information privacy concerns. To comprehensively evaluate the factors influencing VC app use, we proposed and evaluated a conceptual research model based on data collected from 487 professionals. The study sheds light on the role that information privacy concerns, ubiquity, and social presence play in professionals' assessment of perceived benefits and risks. The dual paths of privacy calculus explain the perceived value of VC apps, and ultimately its continuing use.

Although the study makes several theoretical and practical contribution, it is not free of limitations. Our study omitted several important factors that could affect perceived value of VC apps such as perceived fees, synchronicity, system quality, and service quality. A follow up study that includes these factors as

predictors of continuance intention would be beneficial. The collection of the data at a single point in time is arguably another limitation of the study. However, measurement of a specific technology's continuance use is more likely to involve retrospective analysis. Longitudinal studies in the future would be beneficial to determine whether professionals' perceptions of VC apps change over time. Furthermore, data collection for this study was conducted during the COVID-19 pandemic, which may have influenced the study findings. While the research is timely and pertinent to the COVID-19 context, a post-pandemic assessment would be meaningful to determine if the variance explained by the first order and second-order constructs remain unchanged. It would also benefit to longitudinally measure actual usage of VC apps since continuance intention is only a valid predictor of user's post adoption behavior, and mental predisposition is not the equivalent of actual behavior (Bhattacharjee & Barfar, 2011). Lastly, cultural differences influence perceptions of risks and benefits associated with online services (Pentina et al., 2016). We call upon future studies to investigate whether findings from this study hold true for professionals across cultural and geographic boundaries.

References

- Adom, D., Osei, M., & Adu-Agyem, J. (2020). COVID-19 lockdown: A review of an alternative to the traditional approach to research. *Research Journal in Advanced Social Sciences, 1*, 1-9.
- Ahmad, T. (2020). Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. Available at SSRN 3568830.
- Aiken, A. (2020). Zooming in on privacy concerns: Video app Zoom is surging in popularity. In our rush to stay connected, we need to make security checks and not reveal more than we think. *Index on Censorship, 49*(2), 24-27.
- Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods, 18*, 1609406919874596.
- Armfield, N. R., Bradford, M., & Bradford, N. K. (2015). The clinical use of Skype—For which patients, with which problems and in which settings? A snapshot review of the literature. *International Journal of Medical Informatics, 84*(10), 737-742.
- Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Computers in Human Behavior, 58*, 150-157.
- Balasubraman, S., Peterson, R. A., & Jarvenpaa, S. L. (2002). Exploring the Implications of M-Commerce for Markets and Marketing. *Journal of the Academy of Marketing Science, 30*(4), 348-361.
- Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21.
- Barnes, S. J. (2002). Wireless digital advertising: nature and implications. *International journal of advertising, 21*(3), 399-420.
- Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems, 28*(1), 34-49.
- Berezowska, A., Fischer, A. R., Ronteltap, A., van der Lans, I. A., & van Trijp, H. C. (2015). Consumer adoption of personalised nutrition services from the perspective of a risk-benefit trade-off. *Genes Nutr, 10*(6), 42.
- Bhattacharjee, A., & Barfar, A. (2011). Information technology continuance research: current state and future directions. *Asia Pacific Journal of Information Systems, 21*(2), 1-18.

- Billingsley, L. (2020). Using video conferencing applications to share the death experience during the COVID-19 pandemic. *Journal of Radiology Nursing*, 39(4), 275-277.
- Biocca, F., Chad Harms, and Judee K. Burgoon. (2003). Toward a more robust theory and measure of social presence: Review and suggested criteria. *Presence: Teleoperators & virtual environments*, 12(5), 456-480.
- Brewster, T. (2020). Why Zoom really needs better Privacy”: \$1.4 million orders show the US government’s COVID-19 response is now relying on it. <https://www.forbes.com/sites/thomasbrewster/2020/04/02/why-zoom-really-needs-better-privacy-13-million-orders-show-the-us-governments-covid-19-response-is-now-relying-on-it/?sh=5afc61ed77e8>
- Brown, S. A., Dennis, A. R., & Venkatesh, V. (2010). Predicting collaboration technology use: Integrating technology adoption and collaboration research. *Journal of management information systems*, 27(2), 9-54.
- Chin, W. W. (1998). Commentary: Issues and Opinion on Structural Equation Modeling. *MIS quarterly*, 22(1), 7-16. <http://www.jstor.org.proxy.library.vcu.edu/stable/249674>
- Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information systems research*, 14(2), 189-217.
- Chrysochoidis, G., Strada, A., & Krystallis, A. (2009). Public trust in institutions and information sources regarding risk management and communication: towards integrating extant knowledge. *Journal of Risk Research*, 12(2), 137-185.
- Churchill Jr, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of marketing research*, 16(1), 64-73.
- Clarke, D. (2017). End to End Security is Not Enough (Transcript of Discussion). In F. Stajano, J. Anderson, B. Christianson, & V. Matyáš, *Security Protocols XXV Cham*.
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, 10(1), 104-115.
- Degirmenci, K. (2020). Mobile users’ information privacy concerns and the role of app permission requests. *International Journal of Information Management*, 50, 261-272.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, 17(1), 61-80.
- Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of marketing research*, 19(4), 440-452.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 18(1), 39-50.
- Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information systems*, 16(1), 5.
- Goo, J., Kishore, R., Rao, H. R., & Nam, K. (2009). The role of service level agreements in relational management of information technology outsourcing: an empirical study. *MIS quarterly*, 33(1), 119-145.
- Goode, S., Lin, C., Tsai, J. C., & Jiang, J. J. (2015). Rethinking the role of security in client satisfaction with Software-as-a-Service (SaaS) providers. *Decision Support Systems*, 70, 73-85.
- Gray, L. M., Wong-Wylie, G., Rempel, G. R., & Cook, K. (2020). Expanding qualitative research interviewing strategies: Zoom video communications. *The Qualitative Report*, 25(5), 1292-1301.
- Gruzd, A., Staves, K., & Wilk, A. (2012). Connected scholars: Examining the role of social media in research practices of faculty using the UTAUT model. *Computers in Human Behavior*, 28(6), 2340-2350.
- Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, 40(3), 414-433.
- Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage publications.

- Hakim, A. A., Kellish, A. S., Atabek, U., Spitz, F. R., & Hong, Y. K. (2020). Implications for the use of telehealth in surgical patients during the COVID-19 pandemic. *The American Journal of Surgery*, 220(1), 48-49.
- Hamilton, I. A. (2020). Zoom is being Sued for allegedly handing over data to Facebook <https://www.businessinsider.com/zoom-sued-allegedly-sharing-data-with-facebook-2020-3>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135.
- Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In *New challenges to international marketing* (Vol. 20, pp. 277-319). Emerald Group Publishing Limited.
- Jackson, C. B., & Wang, Y. (2018). Addressing the privacy paradox through personalized privacy notifications. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, 2(2), 1-25.
- Johnson, R. E., Rosen, C. C., & Djurdjevic, E. (2011). Assessing the impact of common method variance on higher order multidimensional constructs. *Journal of Applied Psychology*, 96(4), 744.
- Junglas, I., & Watson, R. T. (2006). The u-constructs: four information drives. *Communications of the Association for Information systems*, 17(1), 26.
- Kagan, D., Alpert, G. F., & Fire, M. (2020). Zooming Into Video Conferencing Privacy and Security Threats. *arXiv preprint arXiv:2007.01059*.
- Ke, W., Liu, H., Wei, K. K., Gu, J., & Chen, H. (2009). How do mediated and non-mediated power affect electronic supply chain management system adoption? The mediating effects of trust and institutional pressures. *Decision Support Systems*, 46(4), 839-851.
- Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6), 607-635.
- Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. B. (2016). Limited information and quick decisions: consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction (THCI)*, 8(3), 88-130.
- Kim, H.-W., Chan, H. C., & Gupta, S. (2007). Value-based adoption of mobile internet: an empirical investigation. *Decision Support Systems*, 43(1), 111-126.
- Kim, S., & Garrison, G. (2009). Investigating mobile wireless technology adoption: An extension of the technology acceptance model. *Information Systems Frontiers*, 11(3), 323-333.
- Koch, R. (2020). Using Zoom? Here are the privacy issues you need to be aware of <https://protonmail.com/blog/zoom-privacy-issues/#:~:text=According%20to%20the%20company's%20privacy,using%2C%20and%20your%20IP%20address>
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, 64, 122-134.
- Kordzadeh, N., & Warren, J. (2017). Communicating personal health information in virtual health communities: an integration of privacy calculus model and affective commitment. *Journal of the Association for Information Systems*, 18(1), 1.
- Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: the role of culture. *Business & Information Systems Engineering*, 4(3), 127-135.
- Kumar, P., & Kulkarni, P. (2020). Study of Challenges and Strategies adopted by IT Companies for Internal Customer during COVID-19 Pandemic. *Purakala (UGC Care Journal)*, 31(12), 553-570.
- Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, 33(3), 22-42.
- Lee, G., & Xia, W. (2010). Toward agile: an integrated analysis of quantitative and qualitative field data on software development agility. *MIS quarterly*, 34(1), 87-114.

- Li, C. H., Rajamohan, A. G., Acharya, P. T., Liu, C.-S. J., Patel, V., Go, J. L., Kim, P. E., & Acharya, J. (2020). Virtual read-out: radiology education for the 21st century during the COVID-19 pandemic. *Academic radiology*, 27(6), 872-881.
- Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, 51(1), 62-71.
- Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, 88, 8-17.
- Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the 2012 ACM conference on ubiquitous computing*, 501-510.
- Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, 86(1), 114.
- Linden, A., & Fenn, J. (2003). Understanding Gartner's hype cycles. *Strategic Analysis Report N° R-20-1971. Gartner, Inc*, 88.
- Liu, J. C., & Alexander, R. (2017). Factors affecting faculty use of video conferencing in teaching: A mixed-method study. *Journal of Educational Technology Development and Exchange (JETDE)*, 10(2), 3.
- Maican, C. I., Cazan, A.-M., Lixandroi, R. C., & Dovleac, L. (2019). A study on academic staff personality and technology acceptance: The case of communication and collaboration applications. *Computers & Education*, 128, 113-131.
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4), 336-355.
- Mirzamohammadi, S., & Sani, A. A. (2018). Viola: Trustworthy sensor notifications for enhanced privacy on mobile systems. *IEEE Transactions on Mobile Computing*, 17(11), 2689-2702.
- Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, 47, 120-130.
- Neustaedter, C., Jones, B., O'Hara, K., & Sellen, A. (2018). The Benefits and Challenges of Video Calling for Emergency Situations. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1-13.
- Neustaedter, C., Pang, C., Forghani, A., Oduor, E., Hillman, S., Judge, T. K., Massimi, M., & Greenberg, S. (2015). Sharing domestic life through long-term video connections. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 22(1), 1-29.
- O'Hara, K., Black, A., & Lipson, M. (2009). Media spaces and mobile video telephony. *Media space 20+ years of mediated life*, 303-323.
- Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of advertising*, 38(4), 63-77.
- Okazaki, S., & Mendez, F. (2013). Perceived ubiquity in mobile services. *Journal of Interactive marketing*, 27(2), 98-111.
- Okazaki, S., Molina, F. J., & Hirose, M. (2012). Mobile advertising avoidance: exploring the role of ubiquity. *Electronic Markets*, 22(3), 169-183.
- Ozturk, A. B., Nusair, K., Okumus, F., & Singh, D. (2017). Understanding mobile hotel booking loyalty: an integration of privacy calculus theory and trust-risk framework. *Information Systems Frontiers*, 19(4), 753-767.
- Park, E. K., & Sundar, S. S. (2015). Can synchronicity and visual modality enhance social presence in mobile messaging? *Computers in Human Behavior*, 45, 121-128.
- Patnaik, S. (2020). Zoom pulls in more than 200 million daily video users during worldwide lockdowns. <https://www.reuters.com/article/us-health-coronavirus-zoom/zoom-pulls-in-more-than-200-million-daily-video-users-during-worldwide-lockdowns-idUSKBN21K1C7>
- Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, 65, 409-419.

- Pillet, J.-C., & Carillo, K. D. A. (2016). Email-free collaboration: An exploratory study on the formation of new work habits among knowledge workers. *International Journal of Information Management*, 36(1), 113-125.
- Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: an assessment. *Journal of management information systems*, 10(2), 75-105.
- Plangger, K., & Montecchi, M. (2020). Thinking beyond privacy calculus: Investigating reactions to customer surveillance. *Journal of Interactive marketing*, 50, 32-44.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879.
- Rogers, P., & Lea, M. (2005). Social presence in distributed group environments: The role of social identity. *Behaviour & Information Technology*, 24(2), 151-158.
- Ryans, A. B. (1974). Estimating consumer preferences for a new durable brand in an established product class. *Journal of marketing research*, 11(4), 434-443.
- Sarwar, B., Zulfiqar, S., Aziz, S., & Ejaz Chandia, K. (2019). Usage of social media tools for collaborative learning: The effect on learning success with the moderating role of cyberbullying. *Journal of Educational Computing Research*, 57(1), 246-279.
- Setterstrom, A. J., Pearson, J. M., & Orwig, R. A. (2013). Web-enabled wireless technology: an exploratory study of adoption and continued use intentions. *Behaviour & Information Technology*, 32(11), 1139-1154.
- Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management*, 45, 44-55.
- Short, J., Williams, E., & Christie, B. (1976). *The social psychology of telecommunications*. Toronto; London; New York: Wiley.
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, 35(4), 989-1015.
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*, 20(2), 167-196.
- Straub, D., & Karahanna, E. (1998). Knowledge worker communications and recipient availability: Toward a task closure explanation of media choice. *Organization science*, 9(2), 160-175.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS quarterly*, 13(2), 147-169.
- Teo, H.-H., Wei, K. K., & Benbasat, I. (2003). Predicting intention to adopt interorganizational linkages: An institutional perspective. *MIS quarterly*, 19-49.
- Van Slyke, C., Shim, J., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 16.
- Venkatesh, M. V., Zhao, J., Profitt, L., & Sen-ching, S. C. (2009). Audio-visual privacy protection for video conference. *2009 IEEE International Conference on Multimedia and Expo*, 1574-1575.
- Wang, C., Teo, T. S., & Liu, L. (2020). Perceived value and continuance intention in mobile government service in China. *Telematics and Informatics*, 48, 101348.
- Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, 36(4), 531-542.
- Watson, R. T., Pitt, L. F., Berthon, P., & Zinkhan, G. M. (2002). U-commerce: expanding the universe of marketing. *Journal of the Academy of Marketing Science*, 30(4), 333-347.
- Wiegard, R.-B., & Breitner, M. H. (2019). Smart services in healthcare: A risk-benefit-analysis of pay-as-you-live services from customer perspective in Germany. *Electronic Markets*, 29(1), 107-123.
- Wu, K., Vassileva, J., Noorian, Z., & Zhao, Y. (2015). How do you feel when you see a list of prices? The interplay among price dispersion, perceived risk and initial trust in Chinese C2C market. *Journal of Retailing and Consumer Services*, 25, 36-46.
- Wu, K., Vassileva, J., Zhao, Y., Zhu, Q., & Fang, J. (2014). The Influence of Price dispersion on Purchase Intention in Chinese Online C2C Market: a Trust Perspective. *PACIS*, 72.

- Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *Proceedings of the International Conference on Information Systems Systems*
- Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. *Proceedings of the International Conference on Information Systems*
- Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1), 42-52.
- Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of management information systems*, 26(3), 135-174.
- Ye, S., Lei, S. I., Shen, H., & Xiao, H. (2020). Social presence, telepresence and customers' intention to purchase online peer-to-peer accommodation: A mediating model. *Journal of Hospitality and Tourism Management*, 42, 119-129.
- Yoo, Y., & Alavi, M. (2001). Media and group cohesion: Relative influences on social presence, task participation, and group consensus. *MIS quarterly*, 25(3), 371-390.
- Yuan, S., Hussain, S. A., Hales, K. D., & Cotten, S. R. (2016). What do they like? Communication preferences and patterns of older adults in the United States: The role of technology. *Educational Gerontology*, 42(3), 163-174.
- Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: a means-end model and synthesis of evidence. *Journal of marketing*, 52(3), 2-22.
- Zhang, K., Liu, W.-L., Locatis, C., & Ackerman, M. (2016). Mobile videoconferencing apps for telemedicine. *TELEMEDICINE and e-HEALTH*, 22(1), 56-62.
- Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce*, 16(4), 53-90.
- Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems*, 111(2), 212-226.
- Zhou, T. (2012). Examining mobile banking user adoption from the perspectives of trust and flow experience. *Information Technology and Management*, 13(1), 27-37.