Do Privacy Concerns Determine Online Information Disclosure? The case of Internet Addiction.

Journal:	*Information and Computer Security*
Manuscript ID	ICS-11-2020-0190.R1
Manuscript Type:	Original Article
Keywords:	self-disclosure, Privacy, Information security, social media, SEM, internet addiction

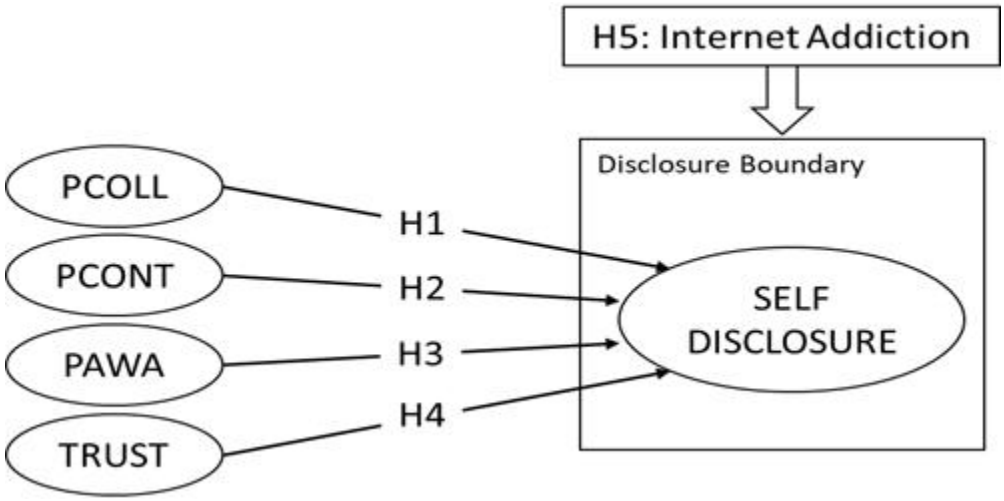

Figure 1: Research Model

175x87mm (72 x 72 DPI)

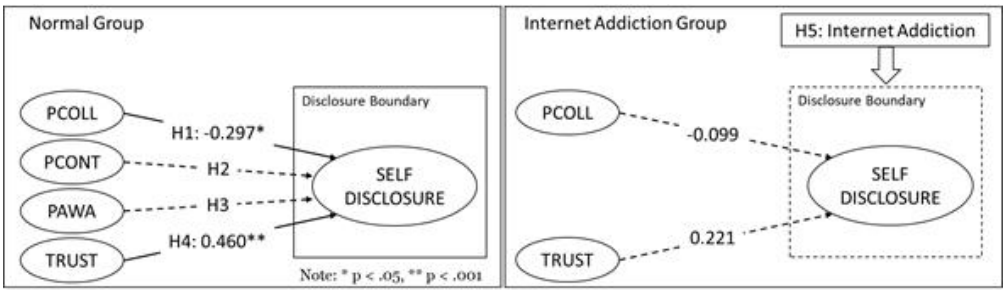

Figure 2. Calculated Model

208x59mm (72 x 72 DPI)

Table 1. Participants

	Level	N	(%)
Gender	Male	108	50.0
	Female	104	48.1
	Other	4	1.9
Age	18-24	58	26.9
	25-34	100	46.3
	35-44	31	14.4
	45+	27	12.5

Table 2. Normal Group

Path	CR	AVE	MSV	1	2	3	4	5
PCOLL	0.882	0.654	0.345	**0.809**				
TRUST	0.839	0.566	0.171	-0.330	**0.752**			
SDIST	0.839	0.571	0.171	-0.279	0.414	**0.756**		
PAWA	0.801	0.575	0.345	0.587	-0.251	-0.022	**0.758**	
PCONT	0.826	0.625	0.192	0.294	-0.264	-0.040	0.438	**0.791**

Table 3. Addiction Group

Path	CR	AVE	MSV	1	2	3	4	5
PCOLL	0.877	0.643	0.221	**0.802**			0	
TRUST	0.864	0.615	0.029	-0.102	**0.784**			
SDIST	0.854	0.594	0.008	0.071	0.089	**0.771**		
PAWA	0.831	0.629	0.581	0.192	-0.171	-0.009	**0.793**	
PCONT	0.748	0.506	0.581	0.470	-0.138	0.035	0.762	**0.712**

Table 4. Multi Group Comparison

Path	**Normal group (n=93)**		**Addiction group (n=123)**		**Significance**
	Path	*SE*	Path	*SE*	
PCOLL	-.297	.150	-.009	.141	p<0.001
TRUST	.460	.116	.221	.127	p<0.001

Do Privacy Concerns Determine Online Information Disclosure? The case of Internet Addiction

Keywords: self-disclosure, privacy, information security, social media, SEM, internet addiction.

Introduction

Much has been written about human factors in the context of information security, privacy, and online behaviours. Often dubbed the "weakest-link" (Schneier 2011), humans have been shown to act non-rationally, and sometimes in ways that contradict their stated views (e.g. Renaud et al. 2016). Prior work demonstrates the crucial role of individual perceptions in guiding behaviours around policy compliance (Bulgurcu, Cavusoglu & Benbasat 2010), privacy behaviours (Kininmonth et al. 2018; Thompson et al. 2020) or home computer security (McGill & Thompson 2017). To address what is a human problem, the popular mechanism of developing successively more complex technology will not suffice. Instead, the root cause must be addressed through behavioural interventions, built upon verified, data-driven models and understanding of human behaviour, and informed by privacy principles (Carron et al. 2016).

Privacy concern vastly pre-dates the internet and modern media (Warren & Brandeis 1890); however, with the advanced and effortless communication that is ubiquitous in modern life, there is potential for far wider privacy harm than ever before. Individuals are subjected to ever-increasing datafication through the widespread aggregation of private social media, internet, travel, or health information. In daily life, individuals also command a far greater audience than previously, with the ability to share with a potential audience of thousands. Furthermore, there is often no effective way to retract information once released. Surprisingly, a hallmark of online privacy research is the inconsistent findings, even when adopting well-known theories such as privacy calculus theory (Jiang, Heng & Choi 2013). Privacy calculus being the assessment made by an individual of the relative costs and benefits of disclosing information (Laufer &

Wolfe 1977). There are clearly many linked forces when it comes to decisions about privacy, and possibly some which may not appear outwardly rational.

The research described in this paper demonstrates one such link – the powerful effect of internet addiction on information disclosure. The observed effect is, in some cases, sufficient to fully negate the influence of privacy concerns. A research model is presented in which three dimensions of privacy concerns are linked to the level of online self-disclosure. The model is tested through multi-group structural equation modelling to reveal the differences between normal vs high internet addiction respondents.

Theoretical Foundation and Research Model

Privacy

Privacy is best understood as being about control in relation to a certain domain, e.g. personal information (Westin 1967). Perceptions of control are inherently subjective and may mean different things depending on the individual or the context. In terms of information privacy, Smith, Milberg and Burke (1996) distilled individuals' general privacy concerns into key dimensions, including the collection of, access to, and unauthorised usage of information. It is these "perceptions about opportunistic behaviour related to the disclosure of personal information submitted over the internet" (Dinev & Hart 2006), that are pertinent in this study. Recognizing that the nature and dimensionality of privacy concerns may have shifted through the widespread adoption of the Internet, later work clarified this dimensionality for an online context by viewing the exchange of information as a form of Social Contract (Dunfee, Smith & Ross Jr 1999). This theory suggests that "*collection* of personally identifiable data is perceived to be fair only when the consumer is granted *control* over the information and the consumer is *informed* about the firm's intended use of the information". This dimensionality has been empirically evaluated showing that in the context of information privacy behaviours, the most influential three factors are: **Factor 1**: *Privacy Concerns of Collection* - An individual's level of concern about concerns about the amount of their data being collected; **Factor 2**: *Privacy Concerns of Control* - An individual's perceived level of control over their personal data

being collected; **Factor 3**: *Privacy Concerns Awareness* - An individual's perceived level of awareness about potential privacy concerns (Malhotra, Kim & Agarwal 2004).

It is generally expected that those who have concerns about how their information will be collected and used will be more cautious and sparing in their level of information disclosure. In other words, those with high privacy concerns will attempt to reduce their exposure by limiting their actions on the internet (Dinev & Hart 2004). The Internet Users Information Privacy Concerns (IUIPC) scale measures privacy concerns in the above domains of collection, control, and awareness (Malhotra, Kim & Agarwal 2004). Building on this prior work, we thus hypothesize:

*H1: Privacy concerns of Collection will **negatively** influence Self-Disclosure*

*H2: Privacy concerns of Control will **negatively** influence Self-Disclosure*

*H3: Privacy concerns Awareness will **negatively** influence Self-Disclosure*

In any interaction where some degree of risk is involved, trust is an influential component (McKnight, Choudhury & Kacmar 2002). While trust may not remove the risk perceptions, it may still operate in an additive manner, thus influencing the strength of the relationships (Dinev & Hart 2006).

Furthermore, we suggest that for those who may not have a well-developed understanding of the concept of privacy, trust serves as a proxy for privacy concerns. Thus, general perceptions of trust may guide users in their disclosure actions. Formally stated, we hypothesize:

*H4: Trust in Social Networks will **positively** influence Self-Disclosure*

Internet Addiction

The increasing usage of the internet in daily life, sometimes even overshadowing other activity, has been of interest within the psychological community. Two decades ago, Young (1998) observed that some online users were becoming addicted in similar ways to that of drugs or alcohol. Although internet addiction was then not formally recognized as a disorder, it shares many traits with those addicted to gambling. This has

been characterised in a few ways, including "pathological internet use" (Davis 2001) or "problematic internet use" (Davis, Flett & Besser 2002). Though these characterisations may be distinct for clinicians, in this research we consider only the fundamental and common traits. That is, that internet addiction can involve compulsive use, is continued despite negative consequences (Cash et al. 2012), and it does not require any intoxicating substance.

In this research, we measure avoidance or distraction behaviour as an indicator of internet addiction. An individual may use the internet as a means of distracting themselves from other important events or tasks in their life. Thus, distraction is a negative state of avoidance-oriented coping (Aladwani & Almarzouq 2016). Avoidance-oriented coping involves behaviour where individuals attempt to avoid dealing directly with stressful situations or events (Holahan et al. 2005). In this case, those using the internet as a distraction seek to forget about other responsibilities. This research is, to our knowledge, the first to explicitly study the effect of internet addiction on the role of privacy perceptions. Hadlington (2017) suggested that individuals who exhibit addictive internet use are more likely to engage in risky security behaviours. Davis, Flett and Besser (2002) empirically showed that distraction is an indicator of internet addiction and validated a measurement scale. Building on this groundwork, we theorise that the internet addict who may be driven by hedonic fulfilment goals toward various types of internet usage may be less rational in their online behaviours. In this context, hedonic goals relate to "fun or pleasure derived from using a technology" (Venkatesh, Thong & Xu 2012, p. 161) which may influence the otherwise rational decisions around online disclosure activity. Thus, any relationships detected between the observed variables and Self-Disclosure will be *weakened* or possibly non-existent. We thus hypothesize that:

H5: Significant influences on Self-Disclosure will be ***weaker*** *for Internet Addicts.*

Causal Model

For consistency with prior work, we present our model (Figure 1) through the lens of privacy calculus theory (Jiang, Heng & Choi 2013). The outcome or dependent variable is the amount of information disclosure on social media, and we predict this is influenced by privacy and trust variables. Privacy concerns

are considered in terms of collection, control, and awareness. Users' each have their own privacy or disclosure boundary, and the extent of their self-disclosure is framed within this boundary (depicted in the research model as a square). We hypothesize that the effect of internet addiction is such that this disclosure boundary is distorted, causing a weakening of any paths which cross it. This is the subject of H5.

<FIG 1 HERE>

Theoretical Foundation and Research Model

Instrument

The research model is composed of 5 constructs. Each construct is measured by multiple items, and all items are drawn from previously validated scales to preserve the content validity. Privacy concerns are considered in terms of three dimensions, which may each influence a users' behaviour, including collection (*PCOLL*), control (*PCONT*) and awareness (*PAWA*) (Hallam & Zanella 2017; Malhotra, Kim & Agarwal 2004). Other constructs modelled are Trust in social networking sites (SNS) (*TRUST*) and Self-Disclosure (*SDISC*) (Contena, Loscalzo & Taddei 2015; Krasnova & Veltri 2011) and Internet Addiction (Davis, Flett & Besser 2002). Items were measured on 7-point Likert scales ranging from Strongly Disagree (1) to Strongly Agree (7). Details of the items in the measurement instrument are provided, along with their sources, in the Appendix.

Participants and Procedure

An online, self-administered questionnaire was developed and distributed by the Qualtrics platform. Participants were required to be over the age of 18 and to consent to participation. The initial distribution of the survey link was made through the researchers' own networks, and snowball sampling was employed. Human Research Ethics Committee approval was obtained before commencing data collection, and this data collection phase concluded in early 2019. At the close of data collection, a total of 263 responses were collected. Incomplete responses or those showing invariance in answering over half of the questions were eliminated, leaving a final usable sample of N=216. Within this sample, 48.1% of respondents were female,

and most respondents were in the 25-34 age bracket. Details of the survey sample are shown below in Table 1.

<TABLE 1 HERE>

Data analysis was conducted with SPSS 25 and AMOS 25 packages for statistical and structural equation modelling. The model was first tested for validity and reliability using confirmatory factor analysis. The resulting model was also tested for Common Method Variance (CMV) before the hypotheses were tested. Finally, a Covariance-Based Structural Equation modelling (CB-SEM) technique was employed using the Maximum Likelihood method of estimation to test the hypotheses. CB-SEM is a second-generation statistical technique which incorporates networks of endogenous and exogenous variables, making it possible to test all relationships simultaneously while controlling for error terms (Hair et al. 1998).

Results and Analysis

Measurement model

All variables were first screened to test the SEM assumptions. Key assumptions were tested by assessing normality and variance inflation factors (VIFs) to reveal any potential collinearity among the constructs in the research model. VIFs were below the most conservative thresholds, and none of the constructs possessed even moderate levels of non-normality. All skewness and kurtosis values were below an absolute value of 1. There were no missing values in the data set. Data were partitioned using a mean split on the internet addiction factor score. This yielded a sample of n=93 normal users and n=123 with above-average internet addiction users. Subsequent analysis was conducted using this grouping.

The research model contains five or fewer constructs, each with more than three items, yielding a target sample size in the region of 100 according to Hair et al (1998). Though our study sample size is n=216, any data partitioning and comparison of groups will bring groups close to this rule of thumb threshold. As the research model is a stable and validated model based on prior work, and there are no missing values, this is a lower concern, however additional sample size calculation was conducted using GPower (Faul et al.

2007). According to this analysis, a minimum sample size of n=87 is required to detect f^2 as low as 0.15 with an achieved power of 85%.

The results of validity and reliability testing are shown in Tables 2 and 3. All the loadings for items in the path model to be tested are above required thresholds indicating a high convergent validity. The composite reliabilities (CR), were all above the required 0.7 threshold (Chin 1998). To evaluate discriminant validity, the square root of the Average Variance Extracted (AVE) for each construct was compared with its intra-construct correlation. Discriminant validity is assured if the square root of the AVE should be higher than the correlation with any other construct. In all but one case, the values on the diagonal (square roots of AVEs) exceed all other values in their respective columns indicating an acceptable level of discriminant validity.

<TABLE 2 HERE>

<TABLE 3 HERE>

Discriminant validity was also tested by calculating the maximum shared variance (MSV) metric and ensuring that these scores are lower than the respective AVE. Once again, this condition was satisfied in all but one case, confirming that the items load more on their respective latent constructs than on any other constructs (Fornell & Larcker 1981). The one case, in which the AVE and MSV test threshold was not met, is in the privacy control (PCONT) construct in the internet addiction group. As shown in Table 4, privacy awareness and privacy control perceptions are highly correlated, leading to a below optimal level of discriminant validity of these constructs. As the data came from a single validated scale, it was not desirable to re-group items into different constructs. Furthermore, the results from an exploratory factor analysis suggested that a different grouping of items would not provide a better overall model fit.

As all data were collected at a single point in time, the threat of common method variance (CMV) was assessed using Harman's single factor test. In this test, exploratory factor analysis was performed, constraining the number of factors to one and with no rotation. The results indicated that CMV was not a

concern in this study since less than 50% of the variance (20.8%) was explained by the single factor (Podsakoff & Organ 1986). Finally, the model fit for the measurement model, including all latent constructs was tested, and found to be excellent ($\chi 2$ / df = 2.178, CFI = 0.919, and SRMR = .069).

Structural Model

The model fit of the structural model was re-tested to ensure that the model fit had not deteriorated and was still in keeping with required thresholds. Figure 2 shows the hypothesis testing results.

<FIG 2 HERE>

For the normal computer users, the model had adequate explanatory power, accounting for 21% of Self-Disclosure variance. H1 and H4 were confirmed. Privacy concerns of Collection (PCOLL) were found to have a significant negative influence on Self-Disclosure (ß = -0.297, $p < .05$). SNS Trust (TRUST) was also found to have a significant positive influence on Self-Disclosure (ß = 0.460, $p < .001$). H2 and H3 were non-significant; neither control nor awareness beliefs regarding privacy have a significant effect on Self-Disclosure.

H5 proposed that any significant relationships may be weaker in the case of internet addiction. Evidence for this was immediately apparent as the two significant paths from the normal user model became non-significant in the internet addiction model. In fact, none of the hypothesized determinants of self-disclosure were significant in the internet addiction group. Further evidence of this effect was found in the R^2 values showing that the model could only account for 3% of the self-disclosure in internet addiction cases. To formally test whether these observed differences in path coefficients were significant, we used the formula of Keil et al. (2000)) Based on this analysis, H5 is accepted as the path coefficients of the two influential paths are significantly different at the $p<0.001$ level. The results of this test are summarized below in Table 4.

<TABLE 4 HERE>

Discussion

We have confirmed the multi-dimensional nature of privacy by separately testing privacy perceptions around collection, awareness, and control of personal data – yielding some new insights. For users with below-average levels of internet addiction, only privacy concerns around *collection* were found to be a significant influence on self-disclosure. This finding is consistent with other recent findings which suggest that the dimension of collection is the most influential determinant of behavioural intentions (Al-Jabri Ibrahim, Eid Mustafa & Abed 2019). That is that those who are generally bothered or think twice about data collection are less likely to self-disclose. Neither privacy concerns *awareness* nor privacy concerns about *control* significantly influenced self-disclosure in this group. This is interesting, given that privacy is commonly defined in terms of control (e.g. Westin 1967). It is likely that, since users are making active and voluntary decisions about the sharing and disclosing of information online, this is not experienced as a loss of control. It is, therefore, not perceived as an interference with privacy.

The role of trust has been confirmed as a strongly influential determinant on self-disclosure. This is consistent with prior work (Krasnova & Veltri 2011). Furthermore, the positive influence of this factor is the strongest of all paths in the model. Although privacy concerns do play a role, it may be the case that more general feelings or perceptions such as those of trust are stronger drivers of user behaviour. For the average user, the biggest determinant of whether the user will disclose private information or not is the level of trust they have in the platform/vendor/entity that is soliciting such information.

When considering the above-average internet addiction group, as hypothesized, there was a measurable effect on the significance of model paths. The two previously significant influences on self-disclosure (H1: Privacy concerns of collection & H4: Trust) were both weakened to the point of no longer being statistically significant. This is consistent with prior theorization on differing goals relating to the hedonic or utilitarian use of technology (Van der Heijden 2004). In this instance, if internet use is to achieve a hedonic goal (in this case distraction from daily tasks or stresses), then external goals (such as protecting one's privacy) may

be de-emphasised. As we present the first work in this area, this signals that this is a promising topic for future research and exploration.

Implications for theory and practice

These findings have several implications for theoreticians and practitioners. Firstly, the role of different privacy dimensions has been clarified. The different dimensions of privacy may be experienced to different degrees by the same user and results show that they do not always influence behaviour. The multidimensionality of privacy is an explanation for the sometimes paradoxical disconnect between stated privacy concerns and behaviour (Kininmonth et al. 2018; Kokolakis 2017). Our work suggests that though the omnibus scales (Smith, Milberg & Burke 1996) are valuable in eliciting broader perspectives in privacy research, they are not suitable for all research goals. Such scales, due to the co-mingling of different dimensions might obscure the specific drivers of user behaviour.

Secondly, it is apparent that, in all users, perceptions about *control* or *awareness* of privacy are not necessarily influential drivers of behaviour. This is relevant for theory building, due to the tradition for privacy to be defined in terms of control. Though this definition is still meaningful, when it comes to online behaviours, users' actions are voluntary, and they may not conflate sharing information with a loss of control. Similarly, the non-significant effect of privacy awareness is relevant for practitioners aiming to improve the security of their users. Organizational interventions around security and privacy are often grounded on the premise that education and awareness is the key to improved cybersecurity (Thomson & von Solms 1998). Security Education, Training and Awareness (SETA) programs that simply attempt to bolster user knowledge, without attempting to understand the motivational factors driving user behaviour may not attain the positive outcomes hoped.

Thirdly, the examination of the role of internet addiction has shown that any previously significant influences on self-disclosure can be overwhelmed. When the usage of any system or service is linked to a hedonic goal, it is valued in terms of the fun or enjoyment of the behaviour (Van der Heijden 2004). For example, although privacy concerns of collection significantly influenced self-disclosure for the normal

user group, for the internet addict, their enjoyment of internet use distorts this relationship. This finding has several implications as it suggests that explanations for any mixed results in prior work may lie in the existence of powerful drivers of human behaviour that have not yet been studied.

Conclusion and Further Research

Increased reliance and usage of modern technology is not universally positive. While technology promises increased productivity, and effortless communication with low cost; its pervasiveness can have negative impacts on the individual and society. Some potential harms to the individual, such as those around privacy, are justifiably receiving attention from the scholarly community. However, there is still much to be learned. This research contributes to a growing body of work in the potential "dark sides of technology" (Tarafdar et al. 2015). As ease-of-access is a factor in developing addictive behaviour (Griffiths & Barnes 2008), it could be that the quest for always-on and always-available technology may have further consequences to the individual.

In this paper, we highlight some of the influences of self-disclosure behaviour, showing that some but not all aspects of privacy are influential. We also provide a first look at the potentially deleterious effect of internet addiction on the rational decision making process of the computer user. This may be one of many unexplored dimensions of human reasoning and decision making. As this research has considered only one element of internet addiction, with promising results, the next step should be to extend the scope of the research with a more comprehensive model. Davis, Flett and Besser (2002) describe four dimensions of internet addiction, these include distraction, impulse control, depression and social comfort. As our research described in this paper has yielded interesting results on the role of distraction, future work may extend the research model to consider further dimensions of internet addiction. We note, however, that although internal validity of these constructs has already been established in prior work, that future researchers must take care to establish external validity as we suggest that not all dimensions of internet addiction will be relevant in a given context. Such future work will be valuable as it may delve deeper into the psychological underpinnings of internet addiction on factors including social comfort and levels of impulse control.

Another valuable step would be to contextualize the work for a specific application domain. For instance, certain applications may likely be perceived by the user as being associated with either work or leisure, and this framing may also ultimately influence behaviour. Unlike computers, which are deterministic, human decisions are influenced by personality, emotions, or hedonic goals. We urge information systems engineers and developers to embrace the role of human factors to create a safer, more efficient and more enjoyable technological environment for all.

References

Al-Jabri Ibrahim, M., Eid Mustafa, I. & Abed, A. 2019, "The willingness to disclose personal information: Trade-off between privacy concerns and benefits", *Information & Computer Security*, Vol. 28, No. 2, pp. 161-81.

Aladwani, A.M. & Almarzouq, M. 2016, "Understanding compulsive social media use: The premise of complementing self-conceptions mismatch with technology", *Computers in Human Behavior*, Vol. 60, pp. 575-81.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS quarterly*, Vol. 34, No. 3, pp. 523-48.

Carron, X., Bosua, R., Maynard, S.B. & Ahmad, A. 2016, "The Internet Of Things And Its Impact On Individual Privacy: An Australian Privacy Principle Perspective", *Computer Law & Security Review*, Vol. 21, No. 1, pp. 4-15.

Cash, H., Rae, C.D., Steel, A.H. & Winkler, A. 2012, "Internet Addiction: A Brief Summary of Research and Practice", *Current psychiatry reviews*, Vol. 8, No. 4, pp. 292-8.

Chin, W.W. 1998, "Commentary: Issues and opinion on structural equation modeling", *MIS quarterly*, Vol. 22, No. 1, pp. vii–xvi.

Contena, B., Loscalzo, Y. & Taddei, S. 2015, "Surfing on Social Network Sites: A comprehensive instrument to evaluate online self-disclosure and related attitudes", *Computers in Human Behavior*, Vol. 49, pp. 30-7.

Davis, R.A. 2001, "A cognitive-behavioral model of pathological Internet use", *Computers in Human Behavior*, Vol. 17, No. 2, pp. 187-95.

Davis, R.A., Flett, G.L. & Besser, A. 2002, "Validation of a new scale for measuring problematic Internet use: Implications for pre-employment screening", *Cyberpsychology & behavior*, Vol. 5, No. 4, pp. 331-45.

Dinev, T. & Hart, P. 2004, "Internet privacy concerns and their antecedents-measurement validity and a regression model", *Behaviour & Information Technology*, Vol. 23, No. 6, pp. 413-22.

—— 2006, "An extended privacy calculus model for e-commerce transactions", *Information systems research*, Vol. 17, No. 1, pp. 61-80.

Dunfee, T.W., Smith, N.C. & Ross Jr, W.T. 1999, "Social contracts and marketing ethics", *Journal of marketing*, Vol. 63, No. 3, pp. 14-32.

Faul, F., Erdfelder, E., Lang, A.-G. & Buchner, A. 2007, "G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences", *Behavior research methods*, Vol. 39, No. 2, pp. 175-91.

Fornell, C. & Larcker, D.F. 1981, "Evaluating structural equation models with unobservable variables and measurement error", *Journal of marketing research*, Vol. 18, No. 1, pp. 39-50.

Griffiths, M. & Barnes, A. 2008, "Internet gambling: An online empirical study among student gamblers", *International Journal of Mental Health and Addiction*, Vol. 6, No. 2, pp. 194-204.

Hadlington, L. 2017, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours", *Heliyon*, Vol. 3, No. 7, pp. 2-18.

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. & Tatham, R.L. 1998, *Multivariate data analysis*, vol. 5, Prentice hall Upper Saddle River, NJ.

Hallam, C. & Zanella, G. 2017, "Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards", *Computers in Human Behavior*, Vol. 68, pp. 217-27.

Holahan, C.J., Moos, R.H., Holahan, C.K., Brennan, P.L. & Schutte, K.K. 2005, "Stress generation, avoidance coping, and depressive symptoms: a 10-year model", *Journal of consulting and clinical psychology*, Vol. 73, No. 4, p. 658.

Jiang, Z., Heng, C.S. & Choi, B.C. 2013, "Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions", *Information systems research*, Vol. 24, No. 3, pp. 579-95.

Keil, M., Tan, B.C., Wei, K.-K., Saarinen, T., Tuunainen, V. & Wassenaar, A. 2000, "A cross-cultural study on escalation of commitment behavior in software projects", *MIS Quarterly*, Vol. 24, No. 2, pp. 299-325.

Kininmonth, J., Thompson, N., McGill, T. & Bunn, A. 2018, "Privacy concerns and acceptance of government surveillance in Australia", paper presented to Proceedings of the 29th Australasian Conference on Information Systems (ACIS 2018), Sydney, Australia, 3-5 Dec.

Kokolakis, S. 2017, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", *Computers & Security*, Vol. 64, pp. 122-34.

Krasnova, H. & Veltri, N.F. 2011, "Behind the curtains of privacy calculus on social networking sites: the study of Germany and the USA", in *Proceedings of the 10th International Conference on Wirtschaftsinformatik*, pp. 891-900.

Laufer, R.S. & Wolfe, M. 1977, "Privacy as a concept and a social issue: A multidimensional developmental theory", *Journal of social Issues*, Vol. 33, No. 3, pp. 22-42.

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*, Vol. 15, No. 4, pp. 336-55.

McGill, T. & Thompson, N. 2017, "Old risks, new challenges: exploring differences in security between home computer and mobile device use", *Behaviour & Information Technology*, Vol. 36, No. 11, pp. 1111-24.

McKnight, D.H., Choudhury, V. & Kacmar, C. 2002, "The impact of initial consumer trust on intentions to transact with a web site: a trust building model", *The journal of strategic information systems*, Vol. 11, No. 3-4, pp. 297-323.

Podsakoff, P.M. & Organ, D.W. 1986, "Self-reports in organizational research: Problems and prospects", *Journal of Management*, Vol. 12, No. 4, pp. 531-44.

Renaud, K., Flowerday, S., English, R. & Volkamer, M. 2016, "Why don't UK citizens protest against privacy-invading dragnet surveillance?", *Information & Computer Security*, Vol. 24, No. 4, pp. 400-15.

Schneier, B. 2011, *Secrets and lies: digital security in a networked world*, John Wiley & Sons.

Smith, H., Milberg, S. & Burke, S. 1996, "Information privacy: Measuring individual's concerns about organizational practices", *MIS quarterly*, Vol. 20, No. 2, p. 167.

Tarafdar, M., DArcy, J., Turel, O. & Gupta, A. 2015, "The dark side of information technology", *MIT Sloan Management Review*, Vol. 56, No. 2, p. 61.

Thompson, N., McGill, T., Bunn, A. & Alexander, R. 2020, "Cultural factors and the role of privacy concerns in acceptance of government surveillance", *Journal of the Association for Information Science and Technology*, Vol. 71, No. 9.

Thomson, M. & von Solms, R. 1998, "Information security awareness: educating your users effectively", *Information Management and Computer Security*, Vol. 6, No. 4, pp. 167-73.

Van der Heijden, H. 2004, "User acceptance of hedonic information systems", *MIS Quarterly*, Vol. 28, No. 4, pp. 695-704.

Venkatesh, V., Thong, J.Y. & Xu, X. 2012, "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology", *MIS quarterly*, pp. 157-78.

Warren, S.D. & Brandeis, L.D. 1890, "The right to privacy", *Harvard law review*, Vol. IV, No. 5, pp. 193-220.

Westin, A.F. 1967, *Privacy and Freedom*, London: The Bodley Head Ltd.

Young, K.S. 1998, "Internet addiction: The emergence of a new clinical disorder", *Cyberpsychology & behavior*, Vol. 1, No. 3, pp. 237-44.

Appendix: Survey Instrument

Construct	Items
PCOLL (Hallam & Zanella 2017; Malhotra, Kim & Agarwal 2004)	It usually bothers me when online companies ask me for personal information. When online companies ask me for personal information, I sometimes think twice before providing it. It bothers me to give personal information to so many online companies. I'm concerned that online companies are collecting too much personal information about me.
PAWA (Hallam & Zanella 2017; Malhotra, Kim & Agarwal 2004)	Companies seeking information online should disclose the way the data is collected, processed, and used. A good SNS online privacy policy should be clear and conspicuous. It is very important to me that I am aware and knowledgeable about how my personal information will be used.
PCONT (Hallam & Zanella 2017; Malhotra, Kim & Agarwal 2004)	Online privacy is really a matter of SNS users' right to exercise control and autonomy over decisions about how their information is collected, used, and shared. SNS users' control of personal information lies at the heart of privacy. I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
TRUST (Contena, Loscalzo & Taddei 2015;	In general, SNS: • are open and receptive to the needs of their members. • make good-faith efforts to address most member concerns. • are honest in their dealings with me. • keep commitments to their members.

Krasnova & Veltri 2011)	
SDISC (Contena, Loscalzo & Taddei 2015; Krasnova & Veltri 2011)	I have a comprehensive profile on social media. I always find time to keep my online profile up-to-date. My profile tells a lot about me. From my social media profile, it would be easy to find out my preferences in music, movies, or books.
ADDICT (Davis, Flett & Besser 2002)	When I have nothing better to do, I go online. I find that I go online more when I have something else I am supposed to do. I sometimes use the Internet to procrastinate. I often use the Internet to avoid doing unpleasant things. Using the Internet is a way to forget about the things I must do but don't want to do.