Global Business and Management Research: An International Journal
Vol. 14, No. 1 (2022)

Impact of Consumer Privacy Concern and Privacy-Related Defensive Behaviour on the Adoption of Social Media Platform

Eng Poh Hwa*
UCSI University, Faculty of Business and Management, Kuala Lumpur, MALAYSIA
Email: engph@ucsiuniversity.edu.my

Tee Wen Sheng
UCSI University, Faculty of Business and Management, Kuala Lumpur, MALAYSIA

** Corresponding Author*

Abstract
Purpose:
The conceptual research aims to investigate the impact of consumer privacy concern and privacy-related defensive behaviour on the adoption of social media platform.
Design/methodology/approach:
This research has adopted systematic literature review, where the systematic literature review is concerned about a research method and process to identify and critically appraising relevant research, to collect and analyse data from the involved research.
Findings: The researchers perform systematic literature review to generate the findings for the conceptual paper. The research develops a theoretical framework using the Power-Responsibility Equilibrium (PRE) theory to explain the phenomenon of privacy concern and privacy-related defensive behaviour.
Research implications:
The research aims to provide insight into how privacy concerns and privacy-related defensive behaviour influence digital marketing in the intensive data-driven field.
Practical implications: The practical implication of this paper is examining privacy concern and privacy-related defensive behaviour, the researchers have adopted the Power-Responsibility Equilibrium (PRE) theory which supported by numerous researchers that conducted similar research in this area. Subsequently, the researchers executed critical literature review to develop the theoretical framework and meanwhile generated fresh insight from the critical analyse.
Originality: The work is an original work which has not been published.

Keywords: Consumer Privacy Concern, Defensive Behaviour, Internet Privacy, Sensitivity, Social Media Platform.

Introduction

The involvement of consumers in the social media platforms has raised the vulnerability associated with information disclosure due to the potential risks of misuse in personal data by ill-intention third parties without obtaining consent form the owners of such information (Arachchilage and love, 2014). Privacy is extremely important for the adoption of social media platforms because a data breach may lead to significant financial loss to consumers when sensitive data are misused by cybercriminals (Ali, 2019).

Privacy is now the most significant challenge for modern life with the increasing dependence on online technology and social media platforms (Durucu et al., 2019). It is important study on the issues relevant to data privacy when social media platforms become more adept to collect and share information, without sufficiently accommodating personal security needs and obligations (Adorjan and Ricciardelli, 2019).

The risk in relevant to protect and maintain consumer data from unauthorised access by the cybercriminals has created vulnerability and detrimental effect on consumers' well-being (Jansen and Van Schaik, 2018). It is evident that the lack of knowledge and awareness of privacy have leaded to vulnerability of consumers (Acquisti et al., 2016). The ability of firms to develop required technology and protocols to maintain privacy, ignoring consumers' psychological state and the behaviour associated with the dilemma on nature and information disclosure have been researched extensively (Barth et al., 2019).

Literature Review

Internet privacy concerns

Internet privacy concerns can be defined as "the degree to which an Internet user is concerned about website practices related to the collection and use of his or her personal information" Hong and Thong (2013, p. 279), which is usually caused by the lack of firms' efforts to protect personal information of users (Buchanan et al. 2007; Culnan and Williams 2009; Pavlou et al. 2007).

Social media privacy concerns refer to the degree to which the users of social media are concerned with a social media site's practices and procedures relating to his or her personal information (Kooang et al., 2018). Privacy concern is defined as individual's extent to protect their personal information and secret matter (Rath & Kumar, 2021). The privacy concern also correlated with privacy risk as people concern about the chance that they poses the privacy risk (Alashoor et al., 2017). In addition, privacy concern can be understood as a cognitive outcome of an individual's tradeoff costs and benefits when disclosing private information (Anderson andAgarwal, 2011). On the other hand, privacy concern can be expressed as a negative attitude toward privacy, when individuals resist allowing their own information to be collected, used and controlled.

Privacy

Privacy can be defined as personal property that reserve right of protection to prevent any disruption from others (Rath & Kumar, 2021). Privacy needs and value in relevant to privacy vary between individuals and depend on an individual's background, experiences, age and gender (Park, 2015).

Privacy can be categorised into two main types 1) physical privacy 2) informational privacy (Moore, 2007). Two main aspects to further segment informational privacy: (1) the right to control one's personal information; (2) the right to prevent access to one's personal information. Users of social media sites are eager to control the information shared online, including contact information, date of birth and full name. They want to control who can access to these information (Birnhack and Elkin-Koren, 2011). Privacy concerns are concerned with social media networks with complex functionalities and advanced capabilities to collect, store and use personal information. For instance, the ability of social media networks to tailor services to individual needs or advertisements to personal preferences (Hong and Thong, 2013).

Privacy concern

There are three major categories of privacy concern that affect users: (1) Notification, many users require to be informed about the collection and use of their personal information by organisations; (2) Control, users require to have control over the collection of their personal information and the sharing of this information among organisations; (3) Security, users require assurance to keep the online stored information safe (Lanier and Saini, 2008). Users are having privacy concern when their information is used without one's permission or when the intended use of the information is unknown (Krafft et al., 2017). In addition, the users' information may be sold to the third parties, without notification to the users about the recipients and usage of the information (Nowak and Phelps, 1995; Phelps et al., 2000).

Users of social media are concerned about their information privacy when their personal information is illegally collected or misused by cybercriminals (Nowak and Phelps, 1997). In addition, users are having privacy concern when they submit their personal information to Web servers voluntarily or involuntarily (Dinev and Hart, 2006).The usage of social media networks requires its users to provide their private data in exchange for a service (Acquisti et al., 2015). Apart from that, social media sites also collect data of its users implicitly by using tracking software or cookies which enable businesses to know consumers' online behaviours and to gather information about their personal preferences and interests (Liu et al., 2004).

The explicit and implicit disclosure of durable private data may lead to different intended or unintended negative consequences to its users despite of the positive intentions for social media sites to connect people, build communities, enhance relationships and share information (Cameron and Webster, 2005). The usage of social media sites usually generates unharmful but potentially annoying impacts including spam messages or personalised advertisements (Prosser, 1960).

In general, there are four serious torts in pertaining to privacy cases including (1) Intrusion, (2) Private Facts, (3) False Light and (4) Appropriation. (1) Intrusion includes the physical or non-physical penetration upon the private sphere of another person in a highly offensive manner. (2) Private Facts describes the publication of highly offensive information about another individual without his or her consent. (3) False Light reflects the false published information. (4) Appropriation involves misuse of another person's data (for instance name) to gain advantage (Prosser, 1960).

In addition, insufficient knowledge or literacy such as the unintentional disclosure of private data or legal prosecution due to improper exposure of information also poses a threat to usage of social media sites (Bartsch and Dienlin, 2016). Apart from that, the storage of data in the digital age is durable that information is undeletable, data collection therefore poses a threat to social media users years after the data collection was done (Mayer-Scho«nberger, 2011).

Social Media Privacy Concern

On the other hand, usage of social media sites exposes its users to potential threats such as heightened vulnerability, personality theft, sexual harassment, opinion manipulation, cyberbullying, fraud, behavioural profiling, unwanted or highly targeted, obtrusive marketing communications and might result in emotional, mental, social, or financial harm to customers and companies alike (Martin and Murphy, 2017).

Researchers found that users of social media sites tend to react to protect their privacy. Users demonstrates a "calculus of behaviour" to evaluate the costs and benefits to provide personal information. Users consider the trade-off between the merits of interactions and potential consequences in attempt to protect their privacy (Laufer and Wolfe, 1977). Users actively engage in withdrawal, defensive behaviour, neutralisation, attack, perception management and reconciliation practices to achieve, maintain and regain control over their personal

domains (Yap et al., 2012).
In addition, there are a variety of online privacy control mechanisms, including separateness, reserve, anonymity, protecting personal information, deception, and dissimulation (Acquisti et al., 2015). Users tend to provide information when they are not personally identified (Cranor et al., 1999). Self-efficacy and demographic factors have different impacts on users' behaviours in using social media sites (Milne et al., 2009). Individual differences including perceptions of user alienation, self-esteem and computer anxiety can directly influence on online privacy concerns (Schwaig et al., 2013). Privacy settings and privacy policy consumption practices play a role to influence users' behaviours in using social media sites (Stutzman et al., 2011).

Defensive behavior towards privacy protection

Privacy concerns trigger the users of social media sites to take measures in protecting their privacy and controlling their private information (Sheng et al., 2008). Therefore, most users share their information with friends and acquaintances. Users opt to control information within the collective privacy boundary through three types of rule management processes to avoid spreading personal information to irrelevant receivers (Petronio, 2002). The three types of rule management processes include permeability (to decide on the amount of private information to disclose), ownership (to decide on who has access to the collective boundary), and linkage (to give permission to share private information) (Petronio, 2002). Users are always precautious in disclosing and sharing of private information with others, for instance, users are more concern about privacy policy and security controls (Milne and Culnan, 2004).

Theoretical Framework

The power responsibility equilibrium is a well-constructed theory to explain the phenomenon of privacy concern and privacy-related defensive behaviour. There is consistent research that applies the theory of power responsibility equilibrium (PRE) to investigate and understand the relationship between consumer privacy and power holder (government sectors and corporate) (Krishen et al., 2017). Indeed, the power responsibility also purposively promotes the balance of social responsibility and social power (Langrehr et al., 1994). The principle of power responsibility equilibrium is to interpret of the influence of corporate business policy and government policy towards privacy concern and privacy-related defensive behaviour. Moreover, the research studies of Schaerer et al., (2018) has highlighted the importance of the balance-power relationship, whereby the power holder should execute the responsibility of using customer personal data in an ethic manner, towards obtain value of equality.
In preciseness the power responsibility equilibrium theory is emphasize on the privacy concern and defensive behaviour from consumer site, and consequently the corporate business policy and government authorities have ability and accountable to protect consumer privacy when misuse occurs (Bandara et al., 2018). Caudill and Murphy (2000) and Lwin et al., (2007) reveal that the privacy-related defensive behaviour is executed by consumer when the privacy protection is missing from government sector. Moreover, the research team from Bandara et al 2021 also conduct empirical research and illustrate the correlation between consumer defensive behaviour and government policies.
In the digital marketing context, there are numerous research studies have been conducted by using the power responsibility equilibrium to explain the privacy concern and defensive behaviour from consumer (Wirtz and Lwin, 2009). In short, after initiating intensive amount of literature review, we decide to apply the power responsibility equilibrium theory to design the theoretical framework to further answer to our research question. Furthermore, this research study is in nature of deductive approach. Hence the numerous research studies show

that the PRE theory is adequate to study privacy concern and privacy-related defensive behaviour (Bandara et al., 2018; Krishen et al., 2017; Lwin et al., (2007).

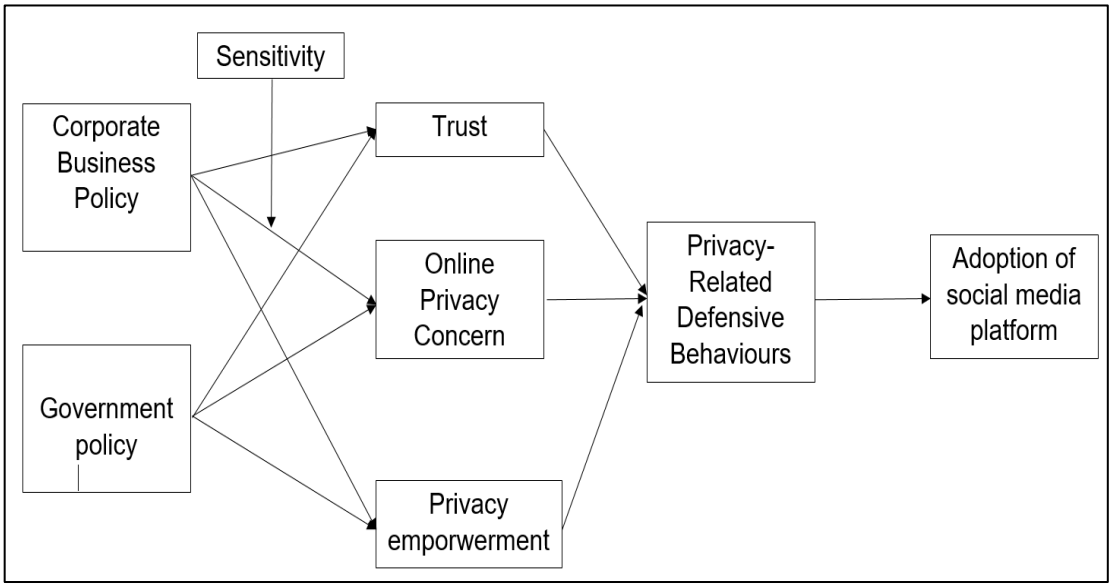

Figure 1: Theoretical Framework

Corporate business policy

The corporate business policy is the independent variable in the research framework. Indeed, the power responsibility equilibrium theory emphasises the influence of power holder on privacy concern (Bandara et al., 2018). Moreover, the research of Krishen et al., (2017) has profound correlations between corporate business policy and consumer privacy concern, by qualitatively examines 322 comments and quantitatively analyse 291 responses in their questionnaire survey. Indeed, the corporate business policy is referred to the initiatives from the corporate site towards providing equality of consumer policy (Culnan & Armstrong, 1999). According to the research study of Pollach (2011) who has illustrated that the business corporate has particular responsibility to the consumer by holding their data for marketing analysis purpose. Furthermore, there is another researcher highlights about the lack of transparency and accountability of corporate policy will lead the consumer to lose trust in the business organisation (Petrescu & Krishen, 2018). Undoubtedly, there are numerous studies have focused on investigating the relationship between corporate business policy and privacy concern, as people perceive the corporate holding certain power to manipulate the privacy of consumer (Petrescu & Krishen, 2018; Lwin et al., 2007; Krishen et al., 2017). On top of that, by examining this factor, the organization could further reconfigure their policy in mitigating the back draws.

Government policy

The government policy refers to regulatory protection initiated by the government sector (Bandara et al., 2018). The government sector has the authority and ability to initiate certain privacy policy that governs the privacy manner on consumer data (Lwin et al., 2007). Furthermore, Miltgen and Smith, (2015) have highlighted in the consumer is expected the government to provide protection to their data, moreover in their empirical research also discuss about the impact of regulation that affects the consumer privacy and behaviour. Furthermore, in the concurrent norm, the consumer is highly relying on social media and meanwhile they are also lacking control and knowledge with privacy issue and data security.

Therefore, the consumer is relying on the legal system and authorities safety mechanisms to protect their personal data (Lwin et al., 2007). Certainly, the investigation of this factor could provide value insight about the influences power from external stakeholder towards consumer privacy concern and privacy-related defensive behaviour.

Trust

Trust is determined as a mediator that affects cooperate business policy and government policy. There are numerous researchers who find that consumer trust has the greatest impact on risk perceptions. The research of van Dyke et al (2007) has focused on the study of the relationship between perceived risk and degree of trust. Furthermore, the consumer trust in a corporate business also will determine the performance of aggregating the consumer data, where the research study find out lack of trust will lead to consumer refuse to share their information (Wirtz and Lwin, 2009). On top of that, the consumer trust in corporate business will influence them whether willing to disclose their personal data and exchange it with a business organisation (Choi et al., 2018). Indeed, if the corporate can guarantee the consumer by will not simply disclose and misuse their data, will increase the trust from consumer to corporate business (Mou et al., 2015).

Online privacy concern

The online privacy concern is a core factor among the whole theoretical framework. The online privacy concern reflects the consumer worries about the misuse of the organisation to their data or discloses their personal data without aware of them (Bandara et al., 2018). Indeed, the privacy concern has been raised in the recent decade, especially when the industry evolution of big data emerged globally. Furthermore, the business corporate not only using consumer data on marketing analyses, besides that, they also selling the consumer data to external parties (Harwin & Gandhi, 2014). Consequently, the awareness of privacy concern will be raised in the recent decade, where consumer unfavourable to see their data be misused by the business organisation. On top of that, the consistent research study on this topic theorised the "privacy concern" to in- depth explain with PRE framework (Lwin et al., 2016; Miltgen et al., 2016; Mousavizadeh et al., 2016). In this study "online privacy concern" reflects the consumer concerns about their privacies in exchange their data with the corporate businesses.

Privacy empowerment

Privacy empowerment is reflected as the belief of consumer that they enjoy the ability to manage their privacy and towards avoiding any unwanted negative outcome (Bandara et al., 2020). Furthermore, there are numerous researchers conducted studies on privacy empowerment (Kucuk, 2016). Indeed, privacy empowerment is considered as consumer's perception of the extent to which control or manage the use of their personal information or use (van Dyke et al., 2007). Moreover, the privacy empowerment would consequently influence the privacy-related defensive behaviour, where the consumer might fabricate, protect or withhold their personal information and refuse exchange with the business organisation (Bandara et al., 2020). On top of that, privacy empowerment is a crucial measurement in this theoretical framework, where it could be driven force to consumer defensive behaviour with protecting their privacy right (Lwin et al., 2016).

Privacy-related defensive behaviour

The defensive behaviour of consumer has been studied immensely by the researchers in the marketing field (Wirtz and Lwin, 2009). The research report of Wirtz and Lwin, (2009) have

provided a definition of defensive behaviour, where they stated that defensive behaviour refers to protecting action initiated by the consumers to prevent the misuse of their personal data or collecting their information by the business organisation. Moreover, this defensive behaviour is associated with privacy concern, according to Krafft et al (2017) illustrate the consumers will only exhibit defensive behaviours when they feel insecure about their privacy are collected by the digital marketer. Furthermore, there are many studies that reveal that defensive behaviours have a mediating effect on the process of aggregate consumer personal data by the business organisation (Bandara et al., 2020). In preciseness, under the PRE theory, the defensive behaviour can be constructed with three exhibitions, namely fabricate, protect and withhold, while those will be implemented by the consumer site (Bandara et al., 2020).

Sensitivity

Sensitivity is a moderator in this research framework. Whereby this is inspired by the research study of Lwin et al., (2007), as they emphasise the congruency-sensitivity interaction has the greatest impact to moderate influence the corporate business policy toward privacy concern. Furthermore, Robbin (2001) find that the consumer is more willing to disclose their personal data when the organisation is asking for insensitive information, for example, general interest. Moreover, there is a profound from another researcher, as their research study have investigated the online privacy concern will be reduced once the required questions are insensitive. On top of that, we think our research study should include this moderator factor to concrete our research analysis.

Method

A systematic literature review is concerned about a research method and process to identify and critically appraising relevant research, to collect and analyse data from the involved research (Liberati et al., 2009). A systematic review aims to identify all empirical evidence that fits the pre-specified inclusion criteria for answering of research question or hypothesis. In addition, through reviewing articles and all available evidence, this method aims to minimise bias and to provide reliable findings from which to make conclusions and decisions (Moher et al., 2009).

The following are the procedures taken to perform the systematic literature review (Saunders et al., 2019).

1 start at a more general level before narrowing down to the specific research question;
2 provide a brief overview of key ideas and themes;
3 summarise, compare and contrast the research of the key authors;
4 narrow down to highlight previous research work most relevant to your own research;
5 provide a detailed account of the findings of this research and show how they are related;
6 highlight those aspects where your own research will provide fresh insights;
7 lead the readers into subsequent sections of the research, which explore these issues.

The backbone of this research paper supported by systematic literature review, to ensure the finding is carries value to the research field. Indeed, we based on the research objective to initiate the systematic literature review by analysing plenty of research finding which relevant to our research objective. As the research objective is to examine privacy concern and privacy-related defensive behaviour, thus we adopted the Power-Responsibility Equilibrium (PRE) theory which supported by numerous researchers that conducted similar research in this area. Subsequently, we executed critical literature review to develop the theoretical

framework and meanwhile generated fresh insight from the critical analyse. The sequences of entire research paper would lead the readers to obtain insight from the board to the specific idea about the research finding.

Discussion and Conclusion

The conceptual research aims to investigate the impact of consumer privacy concern and privacy-related defensive behaviour on the adoption of social media platform. In conclusion, the users of social media platform are very much concerned about the privacy and security in using the social media platforms which trigger to their privacy-related defensive behaviours on the adoption of social media platforms. Therefore, the researchers have adopted the systematic literature review to develop a theoretical framework using the Power-Responsibility Equilibrium (PRE) theory to investigate the impact of consumer privacy concern and privacy-related defensive behaviour on the adoption of social media platform. The research aims to provide insight into how privacy concerns and privacy-related defensive behaviour influence digital marketing in the intensive data-driven field. The conceptual research is an original work, in which it has not published previously.

References

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015). "Privacy and human behavior in the age of information", Science, Vol. 347 No. 6221, pp. 509-514

Acquisti, A., Taylor, C. and Wagman, L. (2016). "The economicsof privacy", Journal of Economic Literature, Vol. 54 No. 2, pp. 442-492.

Adorjan, M. and Ricciardelli, R. (2019). "A new privacy paradox? Youth agentic practices of privacy management despite 'nothing to hide' online", Canadian Review of Sociology/Revue Canadienne de Sociologie, Vol. 56 No. 1, pp. 8-29.

Alderson, P., S.Green, et al. (2004). *Cochrane reviewers' handbook 4.2.2*. In Cochrane Library, Issue 1. Chichester, UK: John Wiley and Sons, Ltd.

Ali, L. (2019). "Cyber-crimes-A constant threat for the business sectors and its growth (A study of the online banking sectors in GCC)", The Journal of Developing Areas, Vol. 53 No. 1, pp. 267-279.

Alkire, L., Pohlmann, J., & Barnett, W. (2019). Triggers and motivators of privacy protection behavior on Facebook. *Journal of Services Marketing*, *33*(1), 57–72. https://doi.org/10.1108/JSM-10-2018-0287

Anderson, C.L. and Agarwal, R. (2011). "The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information", Information Systems Research, Vol. 22 No. 3, pp. 469-490.

Amado, A., Cortez, P., Rita, P., & Moro, S. (2018). Research trends on Big Data in Marketing: A text mining and topic modeling based literature analysis. European Research on Management and Business Economics, 24(1), 1–7. https://doi.org/10.1016/j.iedeen.2017.06.002

Arachchilage, N.A.G. and Love, S. (2014). "Security awareness of computer users: a phishing threat avoidance perspective", Computers in Human Behavior, Vol. 38, pp. 304-312.

Awad, N.F. and Krishnan, M.S. (2006). "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization", MIS Quarterly, Vol. 30 No. 1, pp. 13-28.

Bandara, R., Fernando, M., & Akter, S. (2020). Managing consumer privacy concerns and defensive behaviours in the digital marketplace. European Journal of Marketing, 55(1), 219–246. https://doi.org/10.1108/ejm-06-2019-0515

Bandara, R., Fernando, M., & Akter, S. (2018). Power-Responsibility Dynamics and Consumer Privacy Concerns in the Data-Driven Marketplace. Academy of Management Proceedings, 2018(1), 17669. https://doi.org/10.5465/ambpp.2018.17669abstract

Bartsch, M. and Dienlin, T. (2016). "Control your Facebook: an analysis of online privacy literacy", Computers in Human Behavior, Vol. 56, pp. 147-154.

Barth, S., de Jong, M.D., Junger, M., Hartel, P.H. and Roppelt, J.C. (2019). "Putting the privacy paradox to the test: online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources", Telematics and Informatics, Vol. 41, pp. 55-69.

Benisch, M., Kelley, P.G., Sadeh, N. and Cranor, L.F. (2011). "Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs", Personal and Ubiquitous Computing, Vol. 15 No. 7, pp. 679-694.

Bleier, A., Goldfarb, A., & Tucker, C. E. (2020). Consumer Privacy and the Future of Data-Based Innovation and Marketing. SSRN Electronic Journal. Published. https://doi.org/10.2139/ssrn.3570156

Birnhack, M. and Elkin-Koren, N. (2011). "WikiHunt and the (in) visible handshake", available at: www.opendemocracy.net/michael-birnack-niva-elkin-koren/wikihunt-and-invisible-handshake.

Buchanan, T., Paine, C., Joinson, A.N. and Reips, U.D. (2007). "Development of measures of online privacy concern and protection for use on the internet", Journal of the Association for Information Science and Technology, Vol. 58 No. 2, pp. 157-165.

Caudill, E. M., & Murphy, P. E. (2000). Consumer Online Privacy: Legal and Ethical Issues. Journal of Public Policy & Marketing, 19(1), 7–19. https://doi.org/10.1509/jppm.19.1.7.16951

Cameron, A.F. and Webster, J. (2005). "Unintended consequences of emerging communication technologies: instant messaging in the workplace", Computers in Human Behavior, Vol. 21No. 1, pp. 85-103.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Compañó, R. and Lusoli, W. (2010). "The policy maker's anguish: regulating personal data behavior between paradoxes and dilemmas", in Moore, T., Pym, D. and Ioannidis, C. (Eds), Economics of Information Security and Privacy, Springer, New York, NY, pp. 169-185.

Cranor, L.F., Reagle, J. and Ackerman, M.S. (1999). "Beyond concern: Understanding net users' attitudes about online privacy", in Compaine, B.M. and Vogelsang, I. (Eds) The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy, MIT Press, Cambridge, MA.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science, 10(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Culnan, M.J. and Williams, C.C. (2009). "How ethics can enhance organizational privacy: lessons from the choice point and TJX data breaches", MIS Quarterly, Vol. 33 No. 4, pp. 673-687.

Durucu, M., Isik, M. and Calisir, F. (2019). "What is more important to internet banking website users: usability or functionality?", International Journal ofBusiness Information Systems, Vol. 30 No. 2, pp. 232-251.

Dinev, T. and Hart, P. (2006). "Internet privacy concerns and social awareness as

determinants of intention to transact", International Journal of Electronic Commerce, Vol. 10 No. 2, pp. 7-29.

eBizMBA (2017). "Top 15 most popular social networking sites", available at: www.ebizmba.com/ articles/social-networking-websites (accessed November 7, 2017).

Ellison, N.B., Vitak, J., Gray, R. and Lampe, C. (2014). "Cultivating social resources on social network sites: Facebook relationship maintenance behaviors and their role in social capital processes", Journal of Computer-Mediated Communication, Vol. 19 No. 4, pp. 855-870.

Emerson, R. M. (1964). Power-Dependence Relations: Two Experiments. Sociometry, 27(3), 282. https://doi.org/10.2307/2785619

Eng, P. H., Hamid, S. R., & Chew, B. C. (2020). The adoption of leadership in managing the skilled blue collar workers in the automotive industry in Malaysia in parallel to the industry 4.0. *International Journal of Psychosocial Rehabilitation*, *24*(6), 6194–6207. https://doi.org/10.37200/IJPR/V24I6/PR260625

Equifax (2017). "Equifax security report", available at: www.equifaxsecurity2017.com/consumer-notice/ (accessed September 28, 2017).

Erevelles, S., Fukawa, N. and Swayne, L. (2016). "Big data consumer analytics and the transformation of marketing", Journal of Business Research, Vol. 69 No. 2, pp. 897-904.

Fogel, J. and Nehmad, E. (2009). "Internet social network communities: risk taking, trust, and privacy concerns", Computers in Human Behavior, Vol. 25, pp. 153-60.

Harwin, K., & Gandhi, R. (2014). Digital Green: A Rural Video-Based Social Network for Farmer Training (Innovations Case Narrative: Digital Green). Innovations: Technology, Governance, Globalization, 9(3–4), 53–61. https://doi.org/10.1162/inov_a_00216

Hong, W. and Thong, J.Y. (2013). "Internet privacy concerns: an integrated conceptualization and four empirical studies", MIS Quarterly, Vol. 37 No. 1, pp. 275-298.

Hemp, P. (2006). *Avatar-based marketing. Harvard Business Review*. Harvard Business School Publication.https://sat.xlri.ac.in/sat_ais/resource/resdb/DB10/DB10-2/CBDB102/Avatarbased_Marketing_HBR.pdf

Internet Society (2012). "Global internet user survey 2012", available at: www.internetsociety.org/internet/global-internet-user-survey-2012 (accessed December 10, 2015).

Jansen, J. and Van Schaik, P. (2018). "Testing a model of precautionary online behavior: the case of online banking", Computers in Human Behavior, Vol. 87, pp. 371-383.

Jensen Schau, H., & Gilly, M. C. (2003). We Are What We Post? Self-Presentation in Personal Web Space. Journal of Consumer Research, 30(3), 385–404. https://doi.org/10.1086/378616

Joinson, A.N. (2008). "'Looking at,''Looking up' or 'Keeping up with' people? Motives and uses of Facebook", Proceedings of CHI, ACM, New York, NY, April 05-10.

Kaplan, A. M., & Haenlein, M. (2009). The fairyland of Second Life: Virtual social worlds and how to use them. Business Horizons, 52(6), 563–572.

Kaplan, A. M. (2012). If you love something, let it go mobile: Mobile marketing and mobile social media 4x4. Business Horizons, 55(2), 129–139.

Kietzmann, J., Hermkens, K., McCarthy, I. and Silvestre, B. (2011). "Social media? Get serious! understanding the functional building blocks of social media", Business

Horizons, Vol. 54 No. 3, pp. 241-251.

Kim, D., Ferrin, D. and Rao, H. (2008). "A trust-based consumer decision making model in electronic commerce: the role of trust, perceived risk, and their antecedents", Decision Support Systems, Vol. 44 No. 2, pp. 544-564.

Koohang, A., Paliszkiewicz, J., & Goluchowski, J. (2018). Social media privacy concerns: trusting beliefs and risk beliefs. *Industrial Management and Data Systems*, *118*(6), 1209–1228. https://doi.org/10.1108/IMDS-12-2017-0558

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission Marketing and Privacy Concerns — Why Do Customers (Not) Grant Permissions? Journal of Interactive Marketing, 39, 39–54. https://doi.org/10.1016/j.intmar.2017.03.001

Krishen, A. S., Raschke, R. L., Close, A. G., & Kachroo, P. (2017). A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services. Journal of Business Research, 73, 20–29. https://doi.org/10.1016/j.jbusres.2016.12.002

Kucuk, S. U. (2016). Consumerism in the Digital Age. Journal of Consumer Affairs, 50(3), 515–538. https://doi.org/10.1111/joca.12101

Lanier, C.D. and Saini, A. (2008). "Understanding consumer privacy: a review and future directions", Academy of Marketing Science Review, Vol. 12 No. 2.

Laufer, R.S. and 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.

Liberati, A., Altman, D.G., Tetzlaff, J., Mulrow, C., Gotzshe, P.C., Loannidis, J.P.A., Clarke, M.,Devereaux,P.J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration [e1000100].PLoSMedicine, 6(7),28, https://doi.org/10.1371/journal.pmed.1000100.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. Journal of the Academy of Marketing Science, 35(4), 572–585. https://doi.org/10.1007/s11747-006-0003-3

Liu, Y., Gummadi, K.P., Krishnamurthy, B. and Mislove, A. (2011). "Analyzing Facebook privacy settings: user expectations vs reality", Proceedings ofthe 2011 ACMSIGCOMMConference on Internet Measurement Conference, pp. 61-70.

Liu, C., Marchewka, J.T., Lu, J. and Yu, C.-S. (2005). "Beyond concern – a privacy-trust-behavioral intention model of electronic commerce", Information & Management, Vol. 42 No. 2, pp. 289-304.

Liu, C.,Marchewka,J.T.and Ku,C.(2004). "American and taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce", Journal of Global Information Management,Vol.12No. 1, pp. 18-40.

Lowry, P.B., Cao, J. and Everard, A. (2011). "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures", Journal of Management Information Systems, Vol. 27 No. 4, pp. 163-200.

Madden, M. (2012). "Privacy management on social media sites", Pew Internet Report, Pew Research Center's Internet & American Life Project, Washington, DC, pp. 1-20.

Madejski, M., Johnson, M. and Bellovin, S.M. (2012). "A study of privacy settings errors in an online social network", Proceedings of Pervasive Computing and Communications Workshops, pp. 340-345.

Malhotra, N.K., Kim, S.S. and 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. 336-355.
Martin, K.D. and Murphy, P.E. (2017). "The role of data privacy in marketing", Journal of the Academy of Marketing Science, Vol. 45 No. 2, pp. 135-155.
Mayer-Scho«nberger, V. (2011). Delete: The Virtue ofForgetting in the DigitalAge, Princeton Univ. Press, Princeton, NJ.
Miltgen, C.L., Henseler, J., Gelhard, C. and Popovic, A. (2016), "Introducing new products that affect consumer privacy: a mediation model", Journal of Business Research, Vol. 69 No. 10, pp. 4659-4666
Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. Information & Management, 52(6), 741–759. https://doi.org/10.1016/j.im.2015.06.006
Milne, G.R., Labrecque, L.I. and Cromer, C. (2009). "Toward an understanding of the online consumer's risky behavior and protection practices", Journal of Consumer Affairs, Vol. 43No. 3, pp. 449-473.
Milne, G.R. and Culnan, M.J. (2004). "Strategies for reducing online privacy risks: why consumers read (or don't read) online privacy notices", Journal of Interactive Marketing, Vol. 18 No. 3, pp. 15-29.
Moher D, Liberati A, Tetzlaff J, Altman DG. (2009). Group Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS Med 6: e1000097.
Moynihan, R. (2004). *Evaluating Health Services: A Reporter Covers the Science of Research Synthesis*. New York, Milbank Memorial Fund.
Mou, J., Shin, D. H., & Cohen, J. F. (2015). Trust and risk in consumer acceptance of e-services. Electronic Commerce Research, 17(2), 255–288. https://doi.org/10.1007/s10660-015- 9205-4
Moore, A.D. (2007). "Toward informational privacy rights", The San Diego Law Review, Vol. 44, pp. 809.
Mousavizadeh, M., Kim, D.J. and Chen, R. (2016), "Effects of assurance mechanisms and consumer concerns on online purchase decisions: an empirical study", Decision Support Systems, Vol. 92, pp. 79-90.
Nissenbaum, H. (2015). Respecting Context to Protect Privacy: Why Meaning Matters. Science and Engineering Ethics, 24(3), 831–852.
Nowak, G. and Phelps, J. (1995). "Direct marketing and the use of individual-level consumer infonnation: determining how and when 'privacy' matters", Journal of Direct Marketing, Vol. 9 No. 3, pp. 46-60.
Nowak, G.J. and Phelps, J. (1997). "Direct marketing and the use of individual-level consumer information: determining how and when 'privacy' matters", Journal of Direct Marketing, Vol. 11 No. 4, pp. 94-108
Park, Y.J. (2015). "Do men and women differ in privacy? Gendered privacy and (in)equality in the internet", Computers in Human Behavior, Vol. 50, pp. 252-258.
Pavlou, P.A., Liang, H. and Xue, Y. (2007). "Understanding and mitigating uncertainty in online environments: an agency theory perspective", MIS Quarterly, Vol. 31 No. 1, pp. 105-136.
Pedersen, D.M. (1999). "Model for types ofprivacy by privacy functions", Journal of Environmental Psychology, Vol. 19 No. 4, pp. 397-405.
Petrescu, M. and Krishen, A.S. (2018), "Analyzing the analytics: data privacy concerns", Journal of Marketing Analytics, Vol. 6 No. 2, pp. 41-43.
Petronio, S. (2002). Boundaries ofPrivacy: Dialectics ofDisclosure, State University of New York Press, Albany, NY.

Phelps, J., Nowak, G. and Ferrell, E. (2000). "Privacy concerns and consumer willingness to provide personal information", Journal of Public Policy & Marketing, Vol. 19 No. 1, pp. 27-41.

Pollach, I. (2011). Online privacy as a corporate social responsibility: an empirical study. Business Ethics: A European Review, 20(1), 88–102. https://doi.org/10.1111/j.1467-8608.2010.01611.x

Prescott, M.E. (2014). "Big data and competitive advantage at Nielsen", Management Decision, Vol. 52 No. 3, pp. 573-601.

Prosser, W.L. (1960). "Privacy", California Law Review, Vol. 48No. 3, pp. 383-423.

Robbin, A. (2001). The loss of personal privacy and its consequences for social research. Journal of Government Information, 28(5), 493–527. https://doi.org/10.1016/s1352-0237(02)00343-x

Saunders, M., Lewis, P., and Thornhill, A. (2019). *Research Methods for Business Students* (Eighth Edit.). Pearson Education Limited.

Schaerer, M., du Plessis, C., Yap, A. J., & Thau, S. (2018). Low power individuals in social power research: A quantitative review, theoretical framework, and empirical test. Organizational Behavior and Human Decision Processes, 149, 73–96. https://doi.org/10.1016/j.obhdp.2018.08.004

Schumann, J. H., von Wangenheim, F., & Groene, N. (2014). Targeted Online Advertising: Using Reciprocity Appeals to Increase Acceptance among Users of Free Web Services. Journal of Marketing, 78(1), 59–75. https://doi.org/10.1509/jm.11.0316

Schwaig, K.S., Segars, A.H., Grover, V. and Fiedler, K.D. (2013). "A model of consumers' perceptions of the invasion of information privacy", Information & Management, Vol. 50 No. 1, pp. 1-12.

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. Journal of Advertising, 28(3), 37–51. https://doi.org/10.1080/00913367.1999.10673588.

Sheng, H., Nah, F.F.H. and Siau, K. (2008). "An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns", Journal of the Association for Information Systems, Vol. 9 No. 6, pp. 344-376.

Smith, H.J., Dinev, T. and Xu, H. (2011). "Information privacy research: an interdisciplinary review", MIS Quarterly, Vol. 35 No. 4, pp. 989-1016.

Son, J.Y. and Kim, S.S. (2008). "Internet users' information privacy-protective responses: a taxonomy and a nomological model", MIS Quarterly, Vol. 32 No. 3, pp. 503-529.

SteenKamp, M. and Hyde-Clarke, N. (2014). "The use of Facebook for political commentary in South Africa", Telematics and Informatics, Vol. 31 No. 1, pp. 91-97.

Stutzman, F., Capra, R. and Thompson, J. (2011). "Factors mediating disclosure in social network sites", Computers in Human Behavior, Vol. 27 No. 1, pp. 590-598.

Transfield, D., Denyer, D., Palminder, S. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management* 14, 207-222.

van Dyke, T., Midha, V. and Nemati, H. (2007), "The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce", *ElectronicMarkets*, Vol. 17 No. 1, pp. 68-81.

Wang, L., Hu, H., Yan, J. and Mei, M.Q. (2019). "Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media", Journal of Enterprise Information Management, Vol. 33 No. 2, pp. 353-380.

Westin, A.F. (1968). "Privacy and freedom", Washington and Lee Law Review, Vol. 25 No. 1, pp. 166-170.

Yap, J.E., Beverland, M.B. and Bove, L.L. (2012). "Doing privacy: consumers' search for sovereignty through privacy management practices", Research in Consumer Behavior, Vol. 14, pp. 171-190.

Yadav, M., Joshi, Y., & Rahman, Z. (2015). Mobile Social Media: The New Hybrid Element of Digital Marketing Communications. Procedia - Social and Behavioral Sciences, 189, 335–343. https://doi.org/10.1016/j.sbspro.2015.03.229