Pakistan Journal of Social Research
ISSN 2710-3129 (P) 2710-3137 (O)
Vol. 4, No. 1, March 2022, pp. 511-520.
www.pjsr.com.pk

THE AUDIENCE IS THE KEY, DATA IS NOT: ANALYZING USERS' CONCERNS AND EXPERTS' REFLECTIONS REGARDING PRIVACY POLICIES OF SOCIAL NETWORKING SITES

Madiha Maqsood[*]
PhD Scholar, School of Communication Studies, University of the Punjab Lahore
madiha.ics@pu.edu.pk

Ayesha Ashfaq
Associate Professor, School of Communication Studies, University of the Punjab Lahore

ABSTRACT

The constantly evolving world and the advent of social media gave birth to excessive digitalized human interaction enhancing connectivity among users. These new modes of interaction added to the excitement of sharing, but at the same time it has placed some concerns about the excessive sharing of personal information on digital platforms. The boundaries of subsequent privacy violations are critical concerns in the advance of the technological age. Pakistan is a country with an enormously growing number of internet users, from diverse socio-cultural backgrounds and the platforms are used for distinctive reasons, resulting in millions of posts every minute of the day. A qualitative approach of in-depth interviews was used for the study. Considering the qualitative nature of the study interviews was conducted based on the semi- structured questionnaire. The sample using a purposive sampling technique included users for the sake of highlighting the privacy concerns and experts like media academics, psychologists, lawyers, representatives from the cyber-crime wing of FIA, and the country representatives of social media platforms for understanding the approaches to bridge the gaps regarding those concerns. Social media representatives ensured users' sense of security as a priority of social platforms. Users' inferences and privacy awareness were also gauged which showed concerns about the layout of privacy policies. The privacy calculus approach helped understand the user's psyche of disclosure while having privacy concerns.

Keywords: Social Media, Privacy concerns, Self Disclosure, Privacy Calculus, Privacy policies, Awareness.

INTRODUCTION

The rapid boom of the internet in the 21st century is a key to technological developments globally. The internet has been serving almost one-third of the world's population and is bringing "cross-cultural encounter" opportunities and is revolutionizing communication systems (Ess, 2013). In this way, people are more willing to connect with each other and share their living experiences. Hence, different social mediums provide them with a way to disclose their personal information (Benson et al., 2015). The SNS users access the social sharing sites for free and in exchange for this, they allow those free social networking applications permission to access their data. The data shared by the SNS users are used by the applications for tracking their behavior and for constructing databases containing users' personal data. Many users share their personal data in order to use social applications. As a result, they are more vulnerable to privacy hazards as a result of allowing personal data in the online sphere (Gerber, & Volkamer, 2018) as it is vulnerable to potential privacy risks like increased digital footprints (Litt, 2013) which are used by the third parties and SNS providers (Petkos et al., 2015). While doing online shopping customer trust is a crucial aspect and this counts for the credibility of the source from where they are buying (Pop et al., 2022). This means trust on the platforms plays role in customer choices to buy. Hence, information privacy concern on SNS has become a threat landscape.

Understanding the importance of user privacy, these ideas are now delicately being discussed by researchers. Li et al., (2022) highlighted another aspect of privacy concerns i.e. social media fatigue which according to them mediate the relationship between perceive overload and inert using intentions.

[*] Corresponding Author

In the whole landscape, the audience is the primary stakeholder as they choose which medium to use and how much information is to be allowed. Hence, in order to build a future discourse on this idea, it is very important to understand the dynamics of privacy (Malik, Hiekkanen, & Nieminen, 2016).

According to the Lasswell Formula, scholars from a variety of academic traditions approach the gap differently as digital positivists talk about its ideology (Mosco, 2016). However, the Lasswell Formula somewhat limits the level of thought because of its assumption of the Lasswell Formula, which deals with a set of items like who, when, and with what effect. In general, it misses the role of media in social struggles and power structures as well as the subjectivity, experiences, values, and interpretations of users. According to Fuchs (2017), there is a paradigm shift from digitally driven data analytics to critical social media research, which includes the use of critical realism in social media research methods and ethical considerations. The goal of this research is to better understand the idea of privacy in the context of digital platforms from the perspective of policymakers.

Social Networking Sites and Privacy

During this age of information, the privacy of personal information is becoming a serious ethical issue. Personal information when shared on social networking sites is considered public property. Hence, in addition to the owners of social networking sites, users' personal information is treated as an asset by third parties. The value of such information is increasing day by day and because of technological advancements, the cost of gaining the information is decreasing. In the digital world, information is the currency (K. Zurkus, 2016). These circumstances pose threats to privacy. Hence, as people are becoming more aware of the privacy issues on social networking sites, people have started restricting themselves from sharing their personal information online (Leppäniemi, Karjaluoto, & Saarijärvi, 2017), and hence, it has become difficult to motivate them to do so. They choose self-withdrawal and restrict their online participation because they fear public intrusion in their private lives and hence this is a matter of concern for SNS providers (Krasnova and Veltri, 2010). The current research also aimed at analyzing the self-withdrawal behavior of the users in case they don't feel likely to share their data due to concerns. This is an additional aspect of the privacy calculus approach.

Users Privacy Awareness

It is vital to look at the idea of the privacy paradox but it is more important to know the level of awareness among the users. In the contemporary scenario in which technology is intrusive in everything that users do, millions of consumers are vulnerable to privacy threats. Social networking sites have provided an easy preface to use privacy settings. SNSs privacy settings are flexible for users to choose for themselves whether to be visible to everyone or to custom visibility. These options include family, friends, friends of friends, and the public. But having such provisions the problem exists where people don't change the setting as per their use instead put it as default (Talib et al., 2014). Similarly, Al-Saggaf (2011) stated that even when the privacy policies are clearly mentioned for users about saving and sharing the content they post. But the users do not bother to go through these privacy policies and people rarely get into the details mentioned for safe usage. This gap in the existing literature was sought by the current research as a way of exploring the self-disclosure patterns based on the self-efficacy approach. Users' choices and preferences change as per their social gains. When the gains exceed the loss they go for disclosure anyways (Li, 2012).

Here it is important to raise awareness for safe usage among users of SNS. It could happen by informing them about privacy threats. It makes things clear by telling that online companies depend on collecting large amounts of personal information about users (Zlatolas, Welzer, Hericko, & Hölbl, 2015). Social networks need to have a better analysis of audience ideas for gaining trust which is also a key finding of this study.

SNS users are concerned regarding their privacy when surfing the internet because access to their personal information cannot be controlled which is a threat to privacy (Aimeur, Gambs, and Ho, 2009). But as per Mohamed and Ahmad (2012), users are aware of their privacy protection regarding online threats and they on the basis of their information use those privacy settings to be safe. In their binary study, they developed a new construct of awareness level of privacy policies and validate new self-developed measurement items operationalizing the construct.

Talib et al., (2014) posed the awareness issue in the context of detailed privacy policy provided by SNSs looking at which users can easily comprehend the potential risks of posting information online. According to them when detailed information including technical jargon which is difficult to understand for many users is shared by social platforms users looking at the long details tend to ignore it and instead of reading click agree to continue using without having the idea of potential risk. According to Korzaan and Boswell (2008), the user's concerned behavior about data privacy was considered a key factor that has a positive effect on their behavioral intention to practice privacy protection procedures. The current research also concluded audience awareness is a crucial factor in order to reduce the concerns related to privacy breaches.

Considering the privacy concerns in mind this research seeks to look at experts' reflections and user reviews regarding the privacy policies of Social Networking Sites. The findings contributed towards understanding the practice and bridging the gap between stakeholders in Pakistan by answering the questions of awareness regarding privacy policies among Pakistani University students. Also to what extent the social platforms consider the audience perspective while designing privacy policies, layouts, and other features. As the audience is the key stakeholders hence their mindset, aims, needs and other aspects are considered by SNS platforms.

THEORETICAL FRAMEWORK

The Privacy Calculus Approach

The privacy calculus theory was introduced by Laufer and Wolfe (1977) and is based on privacy management behavior such as self-disclosure decisions (Li, 2012). It highlights how individuals decide to manage their information and whether they should disclose it to others or not (Laufer and Wolfe, 1977). The idea of privacy calculus explains the way individuals exhibit self-disclosure behavior and gives an idea of how they can minimize the negative impact of disclosing their personal information (Li, 2012; Krafft, Arden & Verhoef, 2017).

The Privacy Calculus theory provides a rational analysis in the scenario of privacy (Gomez-Barroso et al., 2018). According to it, before making any choice of disclosing personal information, individuals do a risk-benefit analysis and decide accordingly (Choi, Yi, Jie, & Land, 2018). To determine which aspect is more beneficial, users make an equation by comparing the perceived benefit and the risk of a privacy breach. In comparison with exchange benefits, users consider whether it's fair to disclose personal information (Li, 2012). Users go for self-disclose more in case their gratifications surpass privacy concerns. This means gratifications play a crucial role while making a choice to disclose information (Kezer, Dienlin, & Baruh, 2022).

The concept of privacy calculus is discussed in various aspects just as Motiwalla et al., (2014) focused on the monetary benefit associated with receiving intended products and services. (Lutz, Hoffmann, Bucher, and Fieseler, 2018) The monetary benefit sometimes outweighed the privacy concerns of individuals. For example, coupons were exchanged for personal information (Hallam & Zanella, 2017), or intangible exchange benefits like relationship building, social validation, entertainment, and social capital were exchanged. (Kokolakis, 2017).

The current research aimed at bridging the gap between audience concerns and market practices. Privacy calculus helped understand general audience behavior of disclosure but a few aspects like self-withdrawal and self-efficacy is added to improve the overall context of the privacy comportment.

RESEARCH METHODOLOGY

For this study, a qualitative method of in-depth interviews was used to analyze the audience's perspective and experts' reflections. In-depth interviews provide a way to assess the opinion in detail, in this study in-depth-interviews were conducted using a semi-structured questionnaire. The questionnaire was vet by three field experts and minor changes were incorporated before the interviews were conducted. Keeping in view the qualitative nature of the study interviews were conducted with users, media academics, psychologists, lawyers, representatives from the cyber-crime wing of FIA, and the country representatives of social media platforms using a purposive sampling technique. As reaching out to the experts was a bit difficult so for this study snow ball referral style was also used. Interviews were conducted as per the respondent’s convenience and availability utilizing both face-to-face and online ways. The respondents were sensitized about the research before starting the interviews. Various stakeholders were considered to create a comprehensive image. Interviews were taken unless the responses were exhausted for any further explanations. The user's concerns were studied first before the experts’ reflections were taken. Interviews helped understand the users’ perspectives and expert responses to the concerns rose regarding awareness and privacy policy development.

Table No. 1: Participant of In-depth Interviews

Sr. #	Sample Size	Organizations	No. of Respondents
1.	Country representatives of various major social platforms	Google; Tiktok	2
2.	Representative from the Cyber Crime Wing of FIA	Federal Investigation Agency	1
3.	Digital rights activists	Digital Rights Foundation; Pakistan Software Houses Association for IT and ITES (P@SHA)	2
4.	Psychologist	Institute of Clinical Psychology, University of the Punjab	1
5.	lawyer	Advocate Supreme Court of Pakistan	1
6.	Users	University Students	2
7.	Communication educationalist	Forman Christian College University	1

FINDINGS

4.1. Theme: Awareness regarding privacy policies of the social networks

RQ1 Whether or not Pakistani University students are aware of the privacy policies of the social networks they share information on?

Users ignore the long details of social platforms' guidelines and agree to their terms without even reading them. When asked about whether users care enough about privacy policies, the digital expert narrated, "I think there won't be even a single digit percentage of the people who would be having an idea to maintain their privacy online. People don't even know that apps are free because they are collecting your data."

Another interesting angle is that People are not even aware of the idea of fake news. As explained by the digital expert. People believe whatever they come across on the internet. When they are asked how they have checked the authenticity of news? The usual response is that from Google, Facebook, etc. They are not aware that anyone can post anything on Google and Facebook and hence not all the information on Facebook and Google can be valid. People are unaware of the scenario of how online businesses operate and how they are observed psychologically.

Another digital expert explains it with a general human instinct of ignoring the details. He elaborated on the act by stating that,

> People in Pakistan don't even read the instruction manuals of the appliances. They don't have the habit of reading privacy notices. This is because either they are not taught about these things because Pakistani people are digital immigrants. Even the teaching faculty is not digitally native and there are numerous problems; there are no devices and places for teaching about privacy settings.

When the lawyer was asked about the level of awareness among the people regarding privacy protection, his stance was also consistent with the digital expert he explained the ratio of awareness was as low as 99.99 percent. Cell phones have terms and conditions that state that the owner can even bug the phone and access pictures when the phone is turned on. Even a person living in the USA can take photos with the camera on someone's cell phone, and some social networks use user microphones.

The representative from Tiktok (which is among the most popular apps) said that,

> Users who keep their SNS accounts private stay protected from a mass privacy breach. As there are millions of accounts on SNS, it is possible there is someone who knows you, and they might even know your password if your

> account is hacked. Hence, you need to be very careful about what you share, store and want to keep private.

While discussing ways to increase awareness the digital expert suggested that the users at home, universities, and at a societal level should be provided basic awareness of privacy before giving them cell phones. Whereas the TikTok representative was of the view that awareness campaigns must be organized, the problem is to figure out who is already aware and who requires that awareness. As SNS users must know that they should avoid posting anyone's picture without taking their consent. It is difficult to figure out who needs to know this because generally, a majority knows that taking consent before posting anyone else's picture is an ethical requirement. Hence, the things you won't be doing in the physical world, you should avoid in the digital realm too.

Having said that, spreading awareness of the people who violate the laws and getting punished for it can deter them from violating them in the future. Hence, ignorance cannot be taken as an excuse because it is still wrong whether you know or you don't know.

The researcher asked the audience for their take on whether they read the privacy policies of social networking sites before agreeing to the privacy notices. One of the female respondents said that she reads privacy policies but the issue she faces is that users are bound to accept these policies whether they like them or not. There is no way they can disagree with the policies. Hence she further told that earlier she had limited knowledge but now she reads the privacy policies and understands these things to see how she can deal with the content.

Normally, SNS users find privacy policies way too long and difficult to read so they agree to them without reading the policies. When a Google representative was asked that do people really read privacy policies? He said,

> If I talk about myself, then I accept the privacy policy; I mean a person like me who understands things from a consumer perspective. Within the privacy policies, there exist complexity and it is not easy to make it easier. Like even while signing some legal contract, there is a long notice of 50 pages and we don't even read it properly. We just go through it and sign it.

When the media academics and psychologists were asked about users' approach to privacy policies while downloading applications. They said that users don't read privacy policies because these are written in very small font and too lengthy. Moreover, the privacy policies don't ensure that the personal data is kept confidential, because, in addition to its use for targeting ads, The data is being saved in databases to be sold to third parties. Because there is no such thing as free lunches. A human attention span is 30 sec and you have to decide whether to go through it in 30 sec or not. Hence, people go for comfort and take momentary decisions; they don't read the privacy policy while accepting it and think that they will read in their free time. Moreover, the font of "Agree" is usually larger than the rest of the text, hence motivating the audience to select "Agree" instead of "Don't Agree".

Another aspect stated by the TikTok representative was that:

> People are illiterate and hence they don't know about the guidelines, this is not a healthy situation. Now we have more than 80 billion internet users in this country. Half of the population is on platforms like Facebook, Instagram, Youtube, Tiktok, and Whatsapp. Looking at the education status, they don't support this figure. But, people use these platforms and they understand how to use them. With a little experience, they understand what they are doing there. So, if they post something objectionable, it will get blocked.

Theme: Considering Audience Perspective while designing Policies

RQ2 To what extent do social platforms consider the audience perspective while designing privacy policies, layouts, and other features?

When trends and themes are introduced, the audience's mindset plays a very important role and hence they are the most important asset of social networking sites. Sharing her viewpoint a digital rights activist from Lahore said,

> SNS providers make sure that the audience of their sites feel comfortable and protected. But, some of their policies don't align with what they maintain while talking about providing a protected online sphere.
>
> In terms of what they claim they are looking into, they want to ensure that their users are protected to the greatest extent possible. However, their privacy policies differ according to the culture of different regions, so they don't always suit the circumstances of each country.

When the digital expert having experience working in major social platforms like Twitter, Facebook, Instagram, Youtube, and Google was asked whether the SNS developers keep in mind the audience perspective while developing a theme, he provided a very interesting answer.

> That is actually the only way these companies grow. They made the product so enticing to be used by the consumer. If you are using Instagram, they know how long you scroll, what the things that you like, etc. You use Netflix and you spend the whole night watching it. Do you know what are the competitors of Netflix? A very simple competitor of Netflix is sleep. At the end of each episode, they add some suspense and everyone feels an urge to watch the next episode hence you don't sleep. They are always studying what people like. They are doing research on a massive level. They watch users' behavior, observe people and improve the product. So all digital products are developed taking the audience perspective into consideration. We call this Pull Vs Push; Here pull refers to demand-driven product design.

In addition to this, he elaborated the idea by saying that hundreds of projects are conducted every day around the world to make the apps more user-friendly and interactive. They experimentally design the policies. Product managers on social networking sites are responsible for analyzing product usage and making sure that without spending money on marketing, there is enhanced growth and the audience cannot resist it. Like there is a whole team that analyzes how you respond to "What's on your mind". For example, an experiment was done by writing "Salam, what's on your mind" to a 2% Muslim population and the results were amazing. There are so many similar activities to understand the user approach.

While discussing in the context of regional priorities and differences according to audience demand the digital experts shared that the data collected helps identify the themes of various regions. Giving an example of filters users wanted to have as the first one. The users belonging to Korea, and China wanted to get their features enhanced. The women of Pakistan like filters that cover their hair. Hence, there are specific needs of audience for every region. When people were working on Whatsapp, they did not use the video camera, and when asked why, they answered that we could not turn off the camera from our end; it allows either both cameras to be on or none. To prevent users from turning off the camera, the recommendation was made that the camera should be turned off if they so wish. Hence, product teams in organizations are responsible for improving products.

When the FIA Cyber Crime Wing representative was asked for understanding the user's mindset, and what are the parameters according to which privacy policies are designed; he responded by saying, "The parameters are set by the SNS providers (Facebook, Twitter, WhatsApp, etc.) for the users. These parameters are designed considering the interests of the users and the laws of their respective countries. Security and privacy are two major aspects of these parameters."

The respondents who have exposure to policymaking shared that the privacy policies on SNS might make sure on protecting the data from other people, but your data is still not safe as social media app owners can utilize it in whatever way they want to. It was observed that during the previous US elections, users' data was stolen for election tempering. They influence the users by understanding their temperament, mood, and behaviors. In past years, the nations owning oil wells well dominating the world, but now the people who have an access to the data of the billions of users world was dominated by the people who had oil wells, but now those people are in power who have access to the data of billions of users. Hence, now America and China, the two superpowers, are fighting the wars of data.

Now after realizing the importance of data, China is ready to fight the war with its Tiktok which has taken over American Instagram and Facebook.

The purpose of conducting this research is to look for expert opinions regarding policy development. Hence, a Google representative stated that,

> It was Google that was the first company to move away from using third-party cookies in favor of first-party cookies. Their business model is contrary to anonymizing information, but they are considering it. Rather than focusing on the data, they are focused on the consumer, because they have an idea that the consumer is the most valuable asset they own. Google company has always been a huge survey company, so they conduct surveys and focus groups constantly to learn what people are thinking and doing. Hundreds, if not thousands of surveys on data privacy protection are conducted each month on a regional and global scale.

Users of social sites are more active and observe the changes as they happen. In order to understand what sort of access you are allowing, they now recommend reading the privacy policies. During the installation of the calender application, one user reported that her phone asked for media files, a gallery, and contact information, which she denied considering the potential implications for her privacy.

Similar concerns were raised by other users too. For example, a male user shared that the policies are not in a user-friendly language and are very long and of which users ignore and read them. Most of the users agree without reading and without understanding what they are agreeing with.

Another user stated that:

> People Google things to save time, how can they waste it reading terms and conditions? Hence, if you want people to read the terms and conditions, they should be made user-friendly (short). However, these are not user-friendly. In addition, there are also some technical terms in the privacy policy notice that the majority of the users don't know about. Like people don't know what cookies are. They don't want to improve this; if they want they can improve. This is not a big deal. (User 2)

On this, a TikTok representative while sharing his information on the platforms disclosure policy said:

> A lot of consideration is given to the feedback of customers and consumers, to ensure that the platform is giving the best user experience possible. There are constant surveys being conducted, and many users are unaware that they're taking part. There are times when you are asked to decide whether you like an advertisement or not or whether you want to see more related content or ads that are similar. This is also a part of the feedback research being carried out by the platform.

In extending the discussion, the representative from Google provided an important perspective. He reiterated that privacy is a huge concern at the moment, and Google is a market leader in data protection at the moment. There are huge businesses for third-party cookies and first-party cookies, and both of these are changing all of their fundamentals at a very large and gigantic cost to themselves. They are doing it at a high cost not for themselves but for their consumers.

Previously associated with Facebook and Twitter the representative from the famous social platform Tiktok highlighted that social media platforms in Pakistan adhere to local customers as well. Social media platforms that make them part of the Pakistani community consider certain things to be objectionable that would be perfectly fine in the West. There are certain products you cannot promote in a country like Pakistan; there is a certain kind of imagery that is not allowed in Pakistan even though it is legal in the west.

Table No. 2: for Themes and indicators

Themes	Indicators
1. Awareness regarding privacy policies of the social networks	Role of medium in self-disclosure
	Difficulty in recognizing fake content because of not being digital natives
	Gender and age as indicators of varying privacy awareness
	Lack of interest in privacy based knowledge
	Lack of access for data Forensic
	Agreeing to terms and conditions without reading for the sake of avoiding technical terms and the non-user friendly interfaces
2. Considering Audience Perspective while designing Policies	Varying privacy policies of different regions hence the products and features are developed enticing user's interest
	Social platforms ensure security and privacy as two major aspects
	Pull Vs Push strategy
	Through researches the policies are experimentally design and Audience behavior is gauged through feedback like survey etc.
	Audience is the Key not the data

CONCLUSION

In the age of social media where people have easy access to connect with each other the level of vulnerability has also increased. Users of social networking sites are gradually becoming aware of the hazards but there still is a lot to be done. Even active users also hesitate to read the policy updates and settings. Most of the experts stated that a very small number of users are actually aware of the right usage. There is a need to educate both the heavy and light users regarding safe usage. Audiences are the key to any social medium so they need to do the policy making which is favorable for the users. There is a need to make social media more trustable and user friendly. The SNS providers are making their policies user specific considering the regional perspective. Audience feedback is taken via surveys and experimental approaches after which new themes are implemented. The users' concerns are still there which needs to be addressed for bridging the gap considering security and privacy to be the key aspects of a safe user environment.

Limitations and future prospects

Although this study has provided us with some useful implications in the context of privacy concerns and policy development, some limitations can be addressed through future research. The study is based on a snowball sampling technique; therefore, the results cannot be generalized. Also a quantitative approach in this regard may also help gauge more data which could be generalized. Since this study was limited to the audience awareness and designing privacy policies, a similar study can be carried out using other socio-cultural aspects and their role in the whole process. Relating to the sample, the only required criterion to be selected was to belong from the region of Pakistan either it is a user or an expert having certain exposure with social networking sites. No international experts in this regard were reached out, which is also a limitation of the study. In future a cross cultural study can be conducted to understand the difference of views across regions. Finally, the world of technology is rapidly changing with every day. While this preliminary study may have recognized some of the gaps between users' experiences and policy experts' perspectives, this could help improve the policies of social networking sites especially in the region of Pakistan as per the users' requirements.

REFERENCES

Aimeur, E., Gambs, S., and Ho, A. (2009, May) Upp: User privacy policy for social networking sites. *In 2009 Fourth International Conference on Internet and Web Applications and Services* (pp. 267-272). IEEE.

Al-Saggaf, Y. (2011) Saudi females on Facebook: An ethnographic study. *International Journal of Emerging Technologies and Society*, *9*(1), 1-19.

Benson, V., Saridakis, G., and Tennakoon, H. (2015) Information disclosure of social media users. *Information Technology and People*, *28*, 426 – 441.

Choi, B., Yi, W., Jie, Y., & Land, L. (2018). Love at first sight: The interplay between privacy dispositions and privacy calculus in online social connectivity management. *Journal of The Association for Information Systems*, *19*(3), 124-151. doi:10.17705/1jais.00487

Ess, C. (2013) *Digital Media Ethics.* Retrieved on September 1, 2020 from https://books.google.com.pk/books?hl=enandlr=andid=B23gdgMoBXoCandoi= fndandpg =PT4

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226-261. doi:10.1016/j.cose.2018.04.002

Gómez-Barroso, J. L. (2018) Experiments on personal information disclosure: Past and future avenues. *Telematics and Informatics*, *35*(5), 1473-1490. doi:10.1016/j.tele.2018.03.017

Gómez-Barroso, J. L., Feijóo, C., & Martínez-Martínez, I. J. (2018). Privacy calculus: Factors that influence the perception of benefit. *El profesional de la información (EPI)*, *27*(2), 341-348.

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*, *68*, 217-227. doi:10.1016/j.chb.2016.11.033

Kokolakis, S. (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122- 134. doi:10.1016/j.cose.2015.07.002

Korzaan, M. L., and Boswell, K. T. (2008) The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, *48*(4), 15-24.

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. doi:10.1016/j.intmar.2017.03.001

Krasnova, H., and Veltri, N. F. (2011, February) Behind the curtains of privacy calculus on social networking sites: the study of Germany and the USA. In *10th International Conference on Wirtschaftsinformatik, Zurich, Switzerland* (pp. 891-900).

Kezer, M., Dienlin, T., & Baruh, L. (2022). Getting the privacy calculus right: Analyzing the relations between privacy concerns, expected benefits, and self-disclosure using response surface analysis. Cyberpsychology: *Journal of Psychosocial Research on Cyberspace*, *16*(4), Article 1. https://doi.org/10.5817/CP2022-4-1

Laufer, R. S., and Wolfe, M. (1977) Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*, 22-42. doi: 10.1111/j.1540-4560.1977.tb01880.x

Leppäniemi, M., Karjaluoto, H., & Saarijärvi, H. (2017). Customer perceived value, satisfaction, and loyalty: The role of willingness to share information. *International Review of Retail, Distribution & Consumer Research*, *27*(2), 164. doi:10.1080/09593969.2016.1251482

Li, Y. (2012) Theories in online information privacy research: A critical review and an integrated framework. *Decision support systems*, *54*(1), 471-481.

Li, J., Guo, F., Qu, Q. X., & Hao, D. (2022). How does perceived overload in mobile social media influence users' passive usage intentions? Considering the mediating roles of privacy concerns and social media fatigue. International *Journal of Human–Computer Interaction*, *38*(10), 983-992.

Litt, E. (2013) Understanding social network site users' privacy tool use. *Computers in Human Behavior*, *29*(4), pp. 1649-1656.

Lutz, C., Hoffmann, C. P., Bucher, E., and Fieseler, C. (2018) The role of privacy concerns in the sharing economy. *Information, Communication and Society*, *21*(10), 1472. doi:10.1080/1369118X.2017.1339726

Malik, A., Hiekkanen, K. and Nieminen, M. (2016). Privacy and trust in Facebook photo sharing: age and gender differences. *Program: electronic library and information systems, 50*(4), 462-480. https://doi.org/10.1108/PROG-02-2016-0012

Mohamed, N., and Ahmad, I. H. (2012) Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366-2375.

Mosco, V. (2016) After the internet: Cloud computing, big data and the internet of things. *Les Enjeux de l'information et de la communication*, *2*, 146-155.

Motiwalla, L., Li, X., and Liu, X. (2014) Privacy paradox: Does stated privacy concerns translate into the valuation of personal information? *PACIS 2014 Proceedings*, 281. Retrieved from http://aisel.aisnet.org/pacis2014/281

Petkos, G., Papadopoulos, S., and Kompatsiaris, Y. (2015, August) PScore: a framework for enhancing privacy awareness in online social networks. *In 2015 10th International Conference on Availability, Reliability and Security* (pp. 592-600). IEEE. DOI:10.1109/ARES.2015.80.

Pop, R. A., Săplăcan, Z., Dabija, D. C., & Alt, M. A. (2022). The impact of social media influencers on travel decisions: The role of trust in consumer decision journey. *Current Issues in Tourism, 25*(5), 823-843.

Talib, S., Razak, S. M. A., Olowolayemo, A., Salependi, M., Ahmad, N. F., Kunhamoo, S., and Bani, S. K. (2014, November) Perception analysis of social networks' privacy policy: Instagram as a case study. *In The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M) (pp. 1-5)*. IEEE.

Zlatolas, L. N., Welzer, T., Hericko, M., & Hölbl, M. (2015). Privacy antecedents for SNS ˇ self-disclosure: The case of Facebook. *Computers in Human Behavior, 45*, 158–167.