



Article

Factors Associated with the Privacy Disclosure on Social Media by State University Students in Sri Lanka

C.S.K. Maduragoda^{1,*}, T.U.S. Senarath², and L.I. Manorathne³

1,2. Department of Information Systems, Faculty of Management Studies, Rajarata University of Sri Lanka.

3. Department of English, Faculty of Humanities and Education, CINEC Campus, Millenium Drive, IT Park, Malabe, Sri Lanka.

* Correspondance: chamilsandeep85@gmail.com ;+94 (71) 719 3235

Abstract

The use of social media has become an integral part of the daily life of young people in Sri Lanka. The majority of Sri Lankan youth between the age of 16-25 use social media platforms with Facebook being the most popular one. However, the disclosure of personal information on social media has been associated with various drawbacks, including cyberbullying, identity theft, and physical harm. This research aims to investigate the factors associated with privacy disclosure on social media by state university students in Sri Lanka. The research population consists of undergraduate students from all 17 state universities in Sri Lanka, totalling 327,216 students. The sample is selected using convenience sampling, where 385 undergraduates were selected with a 95% confidence level, and a 5% error rate. The data was collected using a questionnaire and analyzed using statistical procedures such as correlation and multiple regression analysis employing SPSS software. The results of the study reveal that privacy concern was negatively correlated with privacy disclosure, indicating that as privacy concerns increased, students were less likely to disclose personal information on social media. Conversely, perceived benefits were positively correlated with privacy disclosure. These findings suggest that increasing awareness among students of the potential risks associated with sharing personal information online may be an effective measure to prevent privacy disclosure. Furthermore, the study opens avenues for future research to build on its findings and expand understanding of the complex nature of privacy disclosure behavior on social media.

Keywords: privacy disclosure; perceived benefits; privacy concerns; privacy calculus; theory of planned behavior

Article History

Received Date: 29.05.2023

Revised Date: 02.08.2023

Published date: 30.09.2023

1. Introduction

Social media has made a big revolution in the communication process today. There are many social networking sites like Facebook, Instagram, WhatsApp, Viber, etc. People use it as a place to express their thoughts, experiences, images, and even feelings, and it has become an integral part of many people's lives (Sathya & Indradevi, 2017). Social media sites have ingrained itself into everyone's daily lives over the past 20 years, but it is especially prevalent among undergraduates. Students are avid Facebook users, and it's virtually impossible to imagine their life without it (Buzzetto-More, 2012). These include photos, their location, their

relationship status, their education, their contact details, their date of birth, their interests, and their details (Henson et al., 2011). Due to the theft and use of personal information by various groups using the Internet, people using social media have become increasingly concerned about revealing their privacy. Encourage users to submit false information online while discouraging users from disclosing their information (F. Xu et al., 2013). With the growing sustainability of social networking sites, the number of university students who prefer to use social media has been increasing in the last two decades highly. Therefore, millions of people were possible to know about the personal information of all social media users (Athukorala, 2021).

Result of the unauthorized procurement and exploitation of personal information of social media users have been discouraged to support their real, correct information or encouraged to submit their fake, incorrect information to social media (Beigi & Liu, 2020). 2020 Annual Activity Report Sri Lanka CERT mentioned that the majority of reported incidents fell into the category of social media-related occurrences and that there were 15895 of these incidents in 2020 (CERT|CC, 2020). This study was initiated with the goal of presenting a thorough evaluation and analysis of the most recent studies on privacy and disclosure on social media sites. It will also provide an overview of the current studies' locations and key findings, which will aid future researchers in developing new models based on the existing ones. The main objective of this study was to find the factors associated with and their impact on privacy disclosure and Social Media Sites by state university students in Sri Lanka. After reviewing prior literature, it was discovered that several factors have an impact on privacy disclosure. Perceived benefits and privacy concerns are two of those factors. The findings imply that privacy disclosures on social media decrease as privacy concerns increase. On the other hand, privacy disclosures on social media rise as perceived benefits.

2. Literature Review

Social media is an Internet-based channel that allows users to opportunistically interact and selectively self-present, either in real-time or asynchronously, with both broad and narrow audiences who derive value from user-generated content and the perception of interaction with others (Carr & Hayes, 2015). Social networking sites are online platforms that make it easier for people with similar interests, backgrounds, and/or real-world connections to build social networks or social relations. People who sign up for social networking websites build a public profile and connect with their peers. By posting personal details, photos, and interests while creating a profile, they frequently reveal a lot about their actual identity. Information privacy is the interest a person has in being able to control, or at least significantly influence, how information about them is handled. The disclosure of private information via social networking sites may subject users to higher privacy risks (K. Li et al., 2015). Today, personal disclosure is an essential part of developing and maintaining relationships on social media (Tsay-Vogel et al., 2018). Other research shows that even when people express great concern about social media privacy, users are not foolhardy in their disclosure habits, even though some studies reveal that people do little to protect their privacy. Different privacy protection techniques may be used by social media users to address their worries and safeguard their privacy when exposing personal information (Chen, 2018). Identify the four aspects of privacy: the privacy of an individual, the privacy of their behavior, the privacy of their communications, and the privacy of their data. Data privacy and personal communication privacy can both be combined to produce the concept of information privacy (Bélanger & Crossler, 2011). Many concerns about information privacy are fueled by technological advancements. As a result, information systems academics have recently been interested in information privacy. The protection of customer information has grown in importance in online shopping and medical services (Cheng et al., 2021; Malhotra et al., 2004).

When talking about privacy disclosure on social media, more attention should be given to the privacy calculus theory and the reason is that most of the researchers who have been investigated before in this regard have done their investigations using the privacy calculus theory as a grant (Abramova et al., 2017; Cheng et al., 2021; Wang et al., 2017; Wilson & Valacich, 2012; F. Xu et al., 2013). The Privacy Calculus theory explains people consistently analyze the potential benefits and potential risks of data disclosure decisions (Mini, 2019). According to the notion of privacy calculus, when solicited for information in exchange for a good or service, people should do a subjective cost-benefit analysis. Information should only be disclosed when the person believes the advantages will outweigh the dangers of privacy loss (Jozani et al., 2020). The extrinsic factors influencing people's privacy decisions include their subjective perceptions of the advantages of sharing personal information, or perceived benefits (Douglas & Sutton, 2010). By allowing the use of their personal information, social media users can satisfy three needs an information source, leisure, and social interaction, according to research on perceived benefits. Users' access to information services through social media, such as acquiring location information, retrieval information, product list information, and dynamic consultation information, are examples of information sources. Posts, comments, articles, status updates, music, brief films, and other activities that might bring users happiness and pleasure are referred to as leisure. Leisure focuses on the emotional experience of users and includes these types of content. The phrase "social interaction" relates to dialogue and transactions with people and the outside environment, and it particularly refers to social communication traits (Tang et al., 2022).

Privacy concern was identified as one factor that users referred to when considering privacy disclosure on social media (Malhotra et al., 2004). It refers to an individual's worry or anxiety about the unauthorized use of personal information. It can be understood in terms of three dimensions: Awareness, Collection, and Control. Awareness refers to the individual's knowledge of the privacy risks associated with social media. Collection refers to the extent to which individuals are aware of the collection of their personal information by third parties, such as advertisers and data brokers. Control refers to the degree of control that individuals have over their personal information on social media (Lau & Lee, 2012). Studies have shown that privacy concern is a significant factor that influences privacy disclosure on social media (Lin & Lu, 2011; Vosoughi et al., 2018). For example, Vosoughi et al. (2018) found that individuals who have higher privacy concerns are less likely to disclose personal information on social media. Another study, (Lin & Lu, 2011) found that individuals who are more aware of the privacy risks associated with social media are less likely to disclose personal information. These findings suggest that privacy concern plays a significant role in shaping privacy disclosure on social media by state university students in Sri Lanka. It has been demonstrated that privacy concerns in the context of social media negatively affect profile visibility, personal information exposure, self-disclosure, and self-expression. According to recent research, having little faith in other people makes you more worried about their privacy. When privacy concerns are present, low-persistence material would seem to be an important media choice predictor (Choi & Sung, 2018). Information control is the ability of people to manage information that is published online. It has a close connection to having control over one's personal information. People who perceive higher threats to privacy are less disposed to disclosing information about the self and when people perceive lower privacy risks and higher control, they disclose more personal information, because people think that they can't be able to control information when privacy has higher threats and they believe they can control the information when the privacy has fewer risks. The level of privacy concern will be negatively impacted by information control (Taddei & Contena, 2013).

Perceived benefits were also identified as one of the factors that users referred to when considering the privacy disclosure on social media (Malhotra et al., 2004) and it refers to the

positive outcomes that individuals expect to receive from using social media. They can be understood in terms of three dimensions: Information source, Leisure, and social interaction. Information source refers to the extent to which individuals use social media as a source of information. Leisure refers to the extent to which individuals use social media for entertainment and relaxation. Social interaction refers to the extent to which individuals use social media to connect and communicate with others (Lee & Ahn, 2010). Studies have shown that perceived benefits play a significant role in shaping privacy disclosure on social media (Ali et al., 2019). For example, Raza et al. (2019) found that individuals who use social media to connect and communicate with others are more likely to disclose personal information. Another study, Khan & Qureshi (2016) found that individuals who use social media as a source of information are more likely to disclose personal information. These findings suggest that Perceived Benefits play a significant role in shaping privacy disclosure on social media by state university students in Sri Lanka. To balance the perceived risk of the transaction, the other component of the cost-benefit analysis in the privacy calculus entails assessing the perceived benefits of disclosure of personal information. Benefits, when framed inside the privacy calculus model, give the incentive to reveal personal information even when one claims to be concerned about privacy. Wilson & Valacich (2012) The benefit of privacy disclosure has been defined as an individual's sense that providing personal information to a specific transaction partner will result in value. Previous work has found that when users perceive the potential benefits associated with information disclosure, they are more likely to override privacy-related concerns and disclose their personal information in response to value (H. Xu et al., 2011).

The perceived risk of information sharing is inversely related to the perceived benefits of information disclosure. The perceived benefits of information disclosure will be related to perceived privacy. There is a positive relationship between perceived privacy and Perceived benefits of information disclosure. The perceived benefits of information disclosure will be positively correlated with general institutional trust. Perceived benefits and perceived privacy will fully mitigate the impact of general institutional trust on disclosure intention. Increased information sensitivity would lead to an increase in perceived risks and a decrease in perceived benefits, but this impact might be counteracted by positive affect because benefits are overestimated and risks are underestimated (Kehr et al., 2015). Privacy disclosure refers to the extent to which individuals share personal information on social media. It can be understood in terms of three dimensions: Amount, Depth, and Honesty. Amount refers to the quantity of personal information that individuals share on social media. Depth refers to the level of detail of the personal information that individuals share on social media. Honesty refers to the extent to which individuals share accurate and truthful personal information on social media (K. Li et al., 2015).

3. Methodology

3.1 Conceptual Framework

A conceptual framework is a way of conceptualizing how one theorizes a logical sense of the link between the many components that have been recognized as crucial to the problem (Wang et al., 2017). The conceptual framework serves as both the foundation for and the basis for the whole research project. The independent variables of this study were privacy concerns and perceived benefits. The dependent variable of this study was privacy disclosure and those variables were obtained according to privacy calculus theory (X. Li & Chen, 2013). For the aim of this study, the following conceptual framework was provided based on the relationship between research variables (see figure 3).

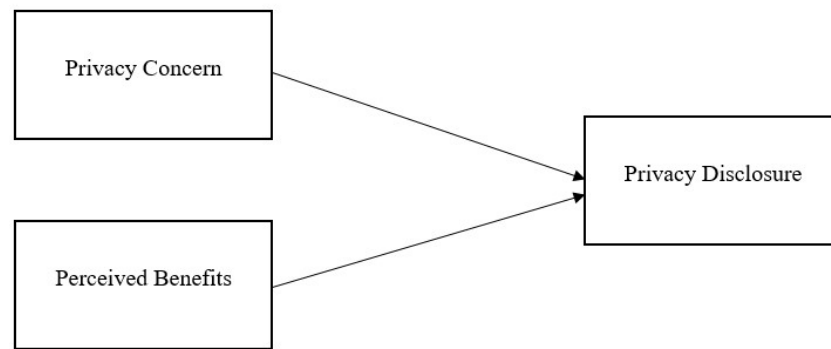


Figure 3. Relationship Between Independent and Dependent Variables

3.2 Population and Sampling

The research population was the undergraduates who are in all 17 state universities in Sri Lanka. There are 327216 students in all these 17 state universities (University Grants Commission, 2021). The sample was selected by using the convenience sampling technique. 385 undergraduates with a 95% confidence level and a 5% error rate are selected as the sample from the population.

$$\text{Sample size} = \frac{\frac{z^2 \times p(1-p)}{e^2}}{1 + \left(\frac{z^2 \times p(1-p)}{e^2 N} \right)}$$

Formula 1. Sample Size Calculation

Where,

N = Population Size,

e = Margin of error (percentage in decimal form),

p = Percentage Value (as a decimal),

z = z- score.

3.3 Reliability and Validity

3.3.1 Reliability

Reliability analysis is an important aspect of research, as it measures the consistency and stability of the data collected. Cronbach's Alpha is a measure of internal consistency, commonly used in research to assess the reliability of a scale or questionnaire. The Cronbach's Alpha value score of 0.7 or higher is generally considered to be acceptable for research purposes. Validity analysis is an essential step in research, as it helps to establish the extent to which the data collected accurately represents the phenomenon being studied. To test for the validity of a study, the Kaiser–Meyer–Olkin (KMO) test, Bartlett's test of sphericity, and

Average Variance Explained (AVE) can be employed. If the value of KMO is greater than 0.5, Bartlett's test of sphericity significant value is less than 0.05, and the AVE value is greater than 0.5 it can be statistically proved that the variables are valid.

Table 1. Test of validity and reliability

Variables	KMO Statistics	Bartlett's test of sphericity significant value	Average Variance Explained (AVE)	Cronbach's Alpha	Number of Questions
Privacy Concern	0.820	0.000	.618	0.784	09
Perceived Benefits	0.838	0.000	.665	0.805	08
Privacy Disclosure	0.839	0.000	.643	0.814	09

According to Table 1, Cronbach's alpha values of all variables ranged from 0.784 to 0.814, which fulfills the relevant accepted level of reliability. Similarly, KMO values of all the variables are ranging from 0.820 to 0.839 which means that all the values are greater than 0.5, significant values of Bartlett's test of sphericity are equal to 0.000 and they are below 0.05, and AVE values of the variables are ranged from 0.618 to 0.665 and all of them are greater than 0.5. That satisfies the requirements of validity and it can be statistically proved that the dimensions and indicators that were used to measure the variables are valid.

4. Results and Discussion

The dependent variable, Privacy Disclosure, was measured using nine questions, and the mean value for this variable was 4.08, with a standard deviation of 0.508. The mean value of 4.08 suggests that, on average, the participants in this study disclose a moderate level of personal information on social media. The standard deviation of 0.508 indicates that the data is relatively consistent, with most participants disclosing personal information within a similar range. The first independent variable, Privacy concern, was measured using nine questions, and the mean value for this variable was 1.87, with a standard deviation of 0.456. The mean value of 1.87 suggests that, on average, the participants in this study have a low level of concern about their privacy on social media. The standard deviation of 0.456 indicates that the data is relatively consistent, with most participants having a similar level of concern about their privacy on social media. The second independent variable, Perceived Benefits, was measured using eight questions, and the mean value for this variable was 4.16, with a standard deviation of 0.512. The mean value of 4.16 suggests that, on average, the participants in this study perceive social media to be highly beneficial. The standard deviation of 0.512 indicates that the data is relatively consistent, with most participants perceiving social media to be highly beneficial.

Table 1. Results of descriptive statistics

	N	Mean	Std. Deviation	Skewness	Kurtosis
	Statistic	Statistic	Statistic	Statistic	Statistic
Privacy Disclosure	385	4.08	.508	-1.304	3.818
Privacy Concerns	385	1.87	.456	1.373	5.425
Perceived Benefits	385	4.16	.512	-1.458	4.810
Valid N (listwise)	385				

Table 2. Results of correlation matrix analysis

		Privacy Disclosure	Privacy Concerns	Perceived Benefits
Privacy Disclosure	Pearson Correlation	1		
	Sig. (2-tailed)			
Privacy Concerns	Pearson Correlation	-.165**	1	
	Sig. (2-tailed)	.001		
Perceived Benefits	Pearson Correlation	.178**	-.189**	1
	Sig. (2-tailed)	.000	.000	

The first independent variable, Privacy concern, had a Pearson correlation value of -0.165 with the dependent variable, Privacy Disclosure (see Table 3). The significant value was 0.001, indicating a statistically significant negative correlation between privacy concerns and privacy disclosure. This means that as privacy concern increases, the tendency for privacy disclosure decreases. In other words, students who are more concerned about their privacy are less likely to disclose personal information on social media. The second independent variable, Perceived Benefits, had a Pearson correlation value of 0.178 with the dependent variable, Privacy Disclosure. The significant value was 0.000, indicating a statistically significant positive correlation between perceived benefits and privacy disclosure. This means that as perceived benefits increase, the tendency for privacy disclosure also increases. In other words, students who perceive social media to be more beneficial are more likely to disclose personal information on social media.

Table 3: Results of regression analysis (Model Summary Table)

Model	R	R Square	Adjusted R Square	Std. Error in the Estimate	Durbin-Watson	Sig.
1	.503 ^a	.255	.250	.397	1.785	.000

In Table 4, the R^2 value indicates how much of the total variation in the dependent variable can be explained by the independent variables. According to the obtained results, the R^2 value is 0.26 and it implies that 25% of the privacy disclosure of the respondents is affected by privacy concerns and perceived benefits and the rest 75% of privacy disclosure is decided by other factors which are explicit to the study while significant value being 0.000 supports the significant relationship between variables.

Table 5. Summary of hypotheses testing

	Hypothesis	Pearson Correlation	Regression
H1	There is an impact of privacy concerns on privacy disclosure on Social Media by State University Students in Sri Lanka	Supported	Supported
H2	There is an impact from perceived benefits on privacy disclosure on Social Media by State University Students in Sri Lanka.	Supported	Supported

According to the both correlation and Regression analysis results first and second hypotheses were supported as shown in the above table (see Table 5).

5. Conclusions

The general objective of this study was to find the associated factors and their impact on the privacy disclosure on social media by state university students in Sri Lanka. By considering the research findings; it can be conveyed that, privacy concerns and perceived benefits are significant predictors of privacy disclosure on social media among state university students in Sri Lanka as most of the previous research concluded. More specifically, privacy disclosure on social media declines as privacy concern rises, representing a significant negative relationship. Meanwhile, privacy disclosure on social media rises as perceived benefits, showcasing a significant positive relationship. The ultimate conclusion was that if university students are more concerned about their privacy on social media, they tend to post fewer things related to their privacy and if they can gain more benefits from social media or if they identify social media as a secure platform with more benefits, they tend to disclose their privacy details on social media.

References

- Abramova, O., Krasnova, H., Wagner, A., & Buxmann, P. (2017). Understanding self-disclosure on social networking sites - a literature review. *AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation, 2017-Augus(May)*.
- Ali, A., Malik, A. K., Ahmed, M., Raza, B., & Ilyas, M. (2019). Privacy concerns in online social networks: A users' perspective. *International Journal of Advanced Computer Science and Applications, 10(7)*, 601–613. <https://doi.org/10.14569/ijacsa.2019.0100780>
- Athukorala, A. W. . (2021). Nature of social media usage by university students in Sri Lanka: A survey. *International Journal of Research and Innovation in Social Science, 05(01)*, 426–432. <https://doi.org/10.47772/ijriss.2021.5130>
- Beigi, G., & Liu, H. (2020). A Survey on Privacy in Social Media. In *ACM/IMS Transactions on Data Science (Vol. 1, Issue 1)*. <https://doi.org/10.1145/3343038>
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly: Management Information Systems, 35(4)*, 1017–1041. <https://doi.org/10.2307/41409971>
- Buzzetto-More, N. A. (2012). Social networking in undergraduate education. *Interdisciplinary Journal of Information, Knowledge, and Management, 7*, 63–90.
- Carr, C. T., & Hayes, R. A. (2015). Social Media: Defining, Developing, and Divining. *Atlantic Journal of Communication, 23(1)*, 46–65. <https://doi.org/10.1080/15456870.2015.972282>
- CERT|CC, S. L. (2020). Annual Activity Report 2020 Sri Lanka CERT | CC The National CERT of.
- Chen, H. T. (2018). Revisiting the Privacy Paradox on Social Media With an Extended Privacy Calculus Model: The Effect of Privacy Concerns, Privacy Self-Efficacy, and Social Capital on Privacy Management. *American Behavioral Scientist, 62(10)*, 1392–1412. <https://doi.org/10.1177/0002764218792691>
- Cheng, X., Hou, T., & Mou, J. (2021). Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing. *Information and Management, 58(6)*, 103450. <https://doi.org/10.1016/j.im.2021.103450>
- Choi, T. R., & Sung, Y. (2018). Instagram versus Snapchat: Self-expression and privacy concern on social media. In *Telematics and Informatics (Vol. 35, Issue 8)*. <https://doi.org/10.1016/j.tele.2018.09.009>

- Douglas, K. M., & Sutton, R. M. (2010). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *European Journal of Social Psychology*, 40(2), 366–374.
- Henson, B., Reynolds, B. W., & Fisher, B. S. (2011). Security in the 21st century: Examining the link between online social network activity, privacy, and interpersonal victimization. *Criminal Justice Review*, 36(3), 253–268. <https://doi.org/10.1177/0734016811399421>
- Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, 107. <https://doi.org/10.1016/j.chb.2020.106260>
- Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6), 607–635. <https://doi.org/10.1111/isj.12062>
- Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information and Management*, 52(7), 882–891. <https://doi.org/10.1016/j.im.2015.07.006>
- Li, X., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Proceedings - 2010 2nd International Conference on Multimedia Information Networking and Security, MINES 2010*, 315–319. <https://doi.org/10.1109/MINES.2010.205>
- Lin, K. Y., & Lu, H. P. (2011). Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in Human Behavior*, 27(3), 1152–1161. <https://doi.org/10.1016/j.chb.2010.12.009>
- Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336–355. <https://doi.org/10.1287/isre.1040.0032>
- Mini, T. (2019). Tobias Mini University of Passau School of Business, Economics and Information Systems Chair of Business Information Systems Reviewer : Advisor : November 2017.
- Sathya, R., & Indradevi, R. (2017). Influence of social media in recruiting talents. *Man in India*, 97(4), 219–231. www.ijsspr.com
- Taddei, S., & Contena, B. (2013). Privacy, trust, and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, 29(3), 821–826. <https://doi.org/10.1016/j.chb.2012.11.022>
- Tang, J., Zhang, B., & Xiao, S. (2022). Examining the Intention of Authorization via Apps: Personality Traits and Expanded Privacy Calculus Perspectives. *Behavioral Sciences*, 12(7). <https://doi.org/10.3390/bs12070218>
- Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media and Society*, 20(1), 141–161. <https://doi.org/10.1177/1461444816660731>
- University Grants Commission. (2021). Detailed undergraduates enrolment of higher educational institutions 2021 - UGC intake. *Detailed undergraduates enrolment of higher educational institutions 2021 - UGC intake*, 47(7), 489–490. <https://doi.org/10.1097/00000446-194707000-00023>

- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. 1151(March), 1146–1151. <https://news.1242.com/article/148290>
- Wang, L., Yan, J., Lin, J., & Cui, W. (2017). Let the users tell the truth: Self-disclosure intention and self-disclosure honesty in mobile social networking. *International Journal of Information Management*, 37(1), 1428–1440. <https://doi.org/10.1016/j.ijinfomgt.2016.10.006>
- Wilson, D. W., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. *International Conference on Information Systems, ICIS 2012*, 5, 4152–4162.
- Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research*, 13(2), 151–168. <https://doi.org/10.1007/s10660-013-9111-6>
- Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Linking Individual Perceptions with Institutional Privacy Assurances Information Privacy Concerns : Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, 12(12), 798–824.