

## Online privacy concerns: A preliminary approach to grasp the privacy concerns of PhD researchers

<b>1<sup>st</sup> Author</b>	<b>Dr.HENRY (Corresponding author)</b> <ul style="list-style-type: none"> <li>• PhD Research Scholar at North Eastern Hill University,Shillong.</li> <li>• Assistant Librarian at Nagaland University, Lumami hqrs.</li> </ul>
<b>2<sup>nd</sup> Author</b>	<b>Dr.JULIE</b> North Eastern Hill University,Shillong.

### Abstract

*Studies have considered the mishandling of personal information that invades online privacy. PhD researchers who constantly visit the Internet for a variety of information sources are also susceptible to these invasive privacy practices by information providers. This investigation tries to understand the privacy perceptions and privacy concerns of PhD researchers in the School of Economics, Management and Information Science at North-Eastern Hill University, India. The results in this paper are based on a statistical analysis of a survey questionnaire administered by hand to the respondents. Descriptive statistics were employed to explore the privacy perception and privacy concerns of the researchers. A closer investigation of the perception towards various privacy issues– revealed that users are highly perceptive towards online privacy violations. While two-thirds of PhD researchers agree that websites can hinder privacy by collecting personal information. Somehow, the majority of (66.7%) of researchers believed their personal information is somewhat protected when seeking information online. Analysis of the study showed high levels of privacy concerns towards financial records like credit cards and identity theft. The results of this study can be helpful in understanding the different perceptions towards online privacy concerns of researchers and in turn, will facilitate the safe use of the Internet when seeking information from the web.*

**Keywords:** *Privacy Concerns, Privacy Perception, Personal Information, Researcher Privacy.*

### 1. Introduction

At present, privacy concerns are becoming an important research area in academia as the absence of online personal information protection leads to putting oneself at risk. Online risks often increase because their personal information is being collected and utilized for unknown purposes (Shin & Kang, 2016). The types of risks that adolescents can be exposed to when they fail to control their own personal information include, but are not limited to, cyberbullying, online stalking, identity theft, identity theft (Cavoukian, 2009). Many studies consider the mishandling of personal information that may invade online privacy concerns is 'data tracking', and 'Identity and financial fraud,' which will be referred to as 'Identity damage' (Lancelot & Smith, 2015). In today's context, users' no longer have control over their

personal information, which has changed people beliefs concerning their online privacy (Martin et al., 2015).

Research has shown that privacy concerns increase as the amount and sensitive personal information submitted through websites increases (Dinev & Hart, 2006). Other privacy issues for students also occurred in numerous ways, such as open access to other students work, public comments, evaluation on critical analysis of students' assignments and work (Chang, 2021). Even though a mechanism is in place to curb privacy violations, users are unaware of the privacy risks associated with disclosing personal information in online environments (Shin & Kang, 2016; Alemany et al., 2019; Tuunainen et al., 2009;Acquisti & Gross, 2006). Therefore, the need to understand privacy concerns and perceptions among PhD researchers' when seeking information from the web becomes more relevant.

While studies have measured online privacy concerns, most of these studies focus only the magnitude of students' privacy concerns (Johns & Lawson, 2005; Gulliver et al., 2015). Thus, it is equally important to investigate researchers' perceptions when they seek information from the web. The lack of empirical research to address the importance of students' attitudes, especially in the region, makes this study valuable and vital to academics and industries. The study will examine the following objectives to gain better insight into researchers' perceptions and concerns.

- 1.1. To understand PhD researcher's perception towards online privacy violations.
- 1.2. To find PhD researcher's perception towards the collected personal information, online banking, unique ID and control belief.
- 1.3. To understand their perception towards search history and protection belief.
- 1.4. To look into their attitude towards different types of privacy concerns.

The article begins with an introduction and objectives. Secondly, a theoretical understanding of privacy concerns and demographic factors with online privacy concerns was discussed. The third part deals with research methodology and measurement items, followed by data analysis and interpretation in the fourth section. The fifth section covers the discussion, and the sixth section discusses the limitation and further studies, which is then followed by a conclusion.

## **2. Literature review**

### **2.1. Privacy concerns**

Privacy concerns have been researched internationally, which indicates that information privacy, which implies "privacy of data," is an important concern to many Internet users. Information privacy laid claims to individuals' personal data not made available to other individuals and organizations. When another party possesses data, the individual must be able to have control over their personal data and its uses (Clarke, 1999). The common legal concept of privacy is often traced back to American scholars Warren and Brandeis' famous essay of 1890 in which they described privacy as "the right to be let alone; the right to liberty" to exercise civil rights over their privacy which includes tangible and intangible (Warren & Brandeis, 1890).

In Westin (1969) work on “Privacy and Freedom”, asked ‘why does a man require privacy at all? Westin finds four human needs that privacy fulfils: solitude, intimacy, anonymity and reserve. Solitude is freedom from observation by others, while intimacy is characterized by a small group of individuals secluded from others to develop their personal relationships. Anonymity is freedom from identification or surveillance in public spaces. Finally, being reserved is limiting disclosure to others so that others know that you are avoiding disclosure. Privacy is a complicated decision problem resulting in opinions, attitudes, and behaviours that differ substantially from one individual to another. The individual perceptions of potential threats, psychological needs, and economic returns all play a role in affecting the decisions to protect or share personal information (Acquisiti & Grossklags, 2005). In addition, different environmental factors (e.g. industry, culture, laws) may also result in differences in perceived privacy concerns (Malhotra et al., 2004).

The ‘secondary usage of information as an aspect of information privacy Culnan (1993) discussed that secondary usage of information occurs when personal data collected for one purpose is then used for a different purpose. While secondary use of data is widespread and legal, it is considered a privacy violation, especially if it occurs without the knowledge or consent of the users. It was discovered that individuals are less likely to perceive these practices as an invasion of privacy if a relationship exists; if an individual has the ability to control the future usage of the information collected, and if the information collected is relevant to the transaction. Tavani’s refer to Internet-specific in privacy studies while arguing that data-mining techniques on the Internet used to gather personal information raises privacy concerns that (a) exceed concerns used in traditional information-retrieval techniques in computer databases and (b) are not taken care of by data-protection laws (Tavani, 1999). The most common theme that emerges is that privacy is a state in which an individual is found in a given situation at a given moment in time (Dinev et al., 2013).

## **2.2. Privacy differences among gender, age and education**

This issue is significant for researchers who are using the Internet consistently to fulfil their academic needs. Privacy is the major concern among major Internet users when using social media, cloud storage, and online banking. With these ever-increasing concerns, users become more aware of the importance of their online privacy. Because of this reason, the perceived risk of Internet users also increased (Lee et al., 2013). Therefore, this may suggest that Internet users’ concerns for privacy issues are triggered when users become aware that organisations or sites have collected and used their personal information without their consent.

The Innovation Diffusion Theory (IDT) of Roger (1983) IDT has assumed that some people are more willing to try innovative ideas and technologies than are others. Rogers (1983) argued that socio-demographic factors such as gender, age, education, and income might determine when individuals adopt innovative ideas and technologies. Various studies have also investigated how demographic differences affect the degree of stated privacy concerns (Chen & Rea, 2004). Privacy concerns are perceived in different online contexts and how socio-demography contributes to understanding privacy concerns (Bergström, 2015).

In the study on ‘Internet users’ perceptions of ‘privacy concerns’ and ‘privacy actions,’ of Paine et al. (2007) reported that a majority of respondents (56%) agreed to be concerned about privacy when they are online, and, this pattern was true for both males and females. While women also tend to have social media profiles for an extended period of time; use

social media more; and tend to be more thoughtful about their social media use, which might explain why previous studies have argued that women tend to feel more concerned than men (Shepherd, 2016).

Some studies have found that online privacy concerns increase with education. For example, Sheehan (2002) four types of online privacy concerns was based on education level and age. So-called (a) “*alarmed internet users*” have the highest level of privacy concerns and tend to have higher levels of education (b) “*wary internet users*” have a moderate level of privacy concerns and tend to be have high levels of education (c) “*circumspect internet users*” have a minimal level of privacy concern and tend to be have lower levels of education, and (d) “*unconcerned internet users*” have the lowest level of privacy concerns and tend to be older and have the lowest levels of education. Notably, it was discovered that age and information privacy concerns have a non-linear relationship. This study confirms that the relationship between gender and information privacy concerns varies with age (Lee et al., 2019). Thus, it may be concluded that as the education level increases, so do their concern over online privacy.

### 3. Methodology

This was a descriptive study that used a survey method to find out the perception of researchers towards online privacy. The study used a questionnaire as the survey instrument.

#### 3.1. Data Collection

A convenient sampling technique was used in the data collection. A total of Forty (40) questionnaires were administered to researchers from the School of Economics, Management and Information Sciences (SEMIS) from North-Eastern Hill University. A total of 30(Thirty) response received from the Department of Library and Information Science; Economics and Commerce of North Eastern Hill University. The survey was distributed through a print questionnaire consisted of multiple questions to suit the study.

#### 3.2. Data Analysis

All the analyses were conducted using IBM SPSS statistics. Descriptive analysis was performed to analyse the researchers' demographic, privacy perceptions and privacy concerns.

#### 3.3. Measurement items

The survey instrument was developed based on validated items, and fewer new items were added to supplement this study. To acquire an insight into the perception of researchers towards ‘privacy violation,’ two statements were presented to them with the response option of ‘Yes’, and ‘No.’ One statement with ‘Yes’, and ‘No,’ responses on online privacy changed with the situation and context was taken from (Kumaraguru & Sachdeva, 2012). For the perception of personal information, online banking, unique ID and control belief, measured on 5-point Likert-type scale (1 = Strongly disagree, 5 = Strongly agree), was adapted from (Kumaraguru and Sachdeva, 2012). Whereby a higher mean score indicates a higher perception. Item was also employed to understand their perception towards search engine personalisation (1 = Not helpful at all, 5 = Extremely helpful) and, for belief in the safety of their personal information when seeking information from the web which were

adapted from Kaiser (2016) on a 5-point Likert-type scale (1 = Less protected, 5 = Very much protected).

The level of privacy concerns consisting of 16 items was measured on a 3-point Likert-type scale ranging from (1 = No concerns at all to 3 = Very concerned) whereby higher mean scores indicated a greater level of privacy concern. These items are ordinal data adapted from attitude items developed by (Buchanan et al., 2007; TRUSTe, 2004).

## 4. Data Analysis and Interpretation

### 4.1. Demographic Sample

A total of (n=30) samples (37% males and 63% females) participated in the survey, with a mean age ( $M = 27.22$ ). Due to the sample population comprising only PhD researchers, there is a lack of age deviation ( $SD = 3.178$ ). Therefore, this demographic factor was not analysed. Respondents from various departments show (Library Science = 40%; Economics = 43% and Commerce at 17%). The finding also revealed that most researchers used the Internet daily (Several times a day = 56.7% and those who always connected = 43.3%).

**4.2. Perceptions towards online privacy violations:** When it comes to understanding the meaning of the term “Online Privacy Issues.” The author allows for multiple selections from the given option, and, hence the finding revealed their understanding of the meaning (Financial scam (n) = 11; Identity theft (n) = 16); Leaking of images and other forms of media (n) = 9; Hacking (n) = 21; Phishing (n) = 7). In **Table 1**, participants were asked whether online privacy changes with situation and context, i.e., the information they share with whom may be different at different times and contexts. The results revealed that 76.7% believed that it changes with the situation and context. A high 93.3% also agreed that their privacy is violated if sites record their online activity without their knowledge. About 73.3% also agreed that their privacy is violated despite agreeing to the site’s privacy policies.

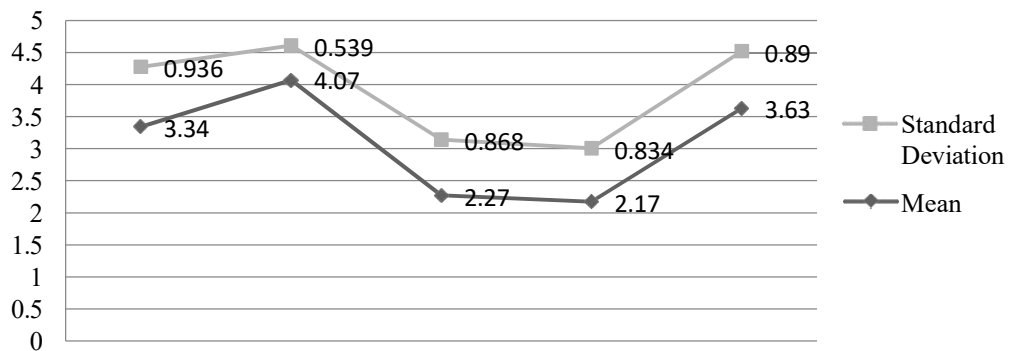
**Table 1.** Perception towards privacy violation

Statements	N		Percent	
	Valid	Missing	Yes (%)	No (%)
Online privacy changed with situation and context	28	2	76.7	16.7
Privacy is violated if sites record my Internet activity without my knowledge	30	0	93.3	6.7
Privacy is violated despite agreeing to privacy policy	29	1	73.3	23.3

**4.3. Perception on personal information, online banking, unique ID and control belief:** To indicate the perception of respondents towards the given statements in **Figure 1**, all five (5) statements were measured on a five-point scale ranging from (1 = Strongly disagree, 5 = Strongly agree). The study showed that more than two-thirds of respondents agree that websites can hinder privacy by collecting personal information ( $M = 4.07$ ,  $SD = 0.539$ ). A high mean score is also recorded in ways Internet users’ lose control over their personal information being circulated to other organizations ( $M = 3.63$ ,  $SD = 0.890$ ). However, respondents also perceived that websites handle their personal information in a confidential way ( $M = 3.34$ ,  $SD = 0.936$ ). It is notable, the mean score for online banking and

unique identification (For instance, Aadhaar ID and Passport ID, etc.) is considerably on the low side, indicating their low agreement on these two statements.

**Figure 1.** Perception on personal information, online banking, unique ID and control belief.



Website handles personal information by our banking, ID, Aadhaar, and other personal information circulated by other organisation.

**Note:** Measured on 5-point Likert item (1 = strongly disagree, 5 = strongly agree).

**4.4. Perception towards search history and protection belief:** While measuring the respondent’s response (see **Table 2**) towards search engine that tracks their search history, and then use that information to personalize their future search results. The finding to this reveal (extremely helpful = 3.3%; helpful = 43.3%; neutral = 40%; not so helpful 13.3%). The result also shows that the majority (66.7%) of respondents believed their personal information is somewhat protected when seeking information online; about (21.4%) believed their personal information is less protected and, only (13.4%) believed they are either protected or significantly protected.

**Table 2.** Perception towards search history and protection belief

Statements	N	M	SD	Not helpful at all (%)	Not Helpful (%)	Neutral (%)	Helpful (%)	Extremely helpful (%)
Perception towards search engine tracking search history and used that information to personalized future search results	30	3.37	.765	0	13.3	40	43.3	3.3
				Less protected (%)	Somewhat protected (%)	Protected (%)	Significantly protected (%)	Very much protected (%)
I believed my personal information is protected while seeking information	28	2	.525	20	66.7	6.7	6.7	0



online								
--------	--	--	--	--	--	--	--	--

**Note:1.** Measured on 5-point Likert type item (1 = Not helpful at all, 5 = Extremely helpful) **2.** Measured on 5-point Likert type item (1 = Less protected, 5 = Very much protected).

**4.5. Different types of privacy concerns:** Based on the level of privacy concerns 16 items built of the eleven statements, the descriptive statistics of these variables are presented in **Table 3**. These items were measured on a three-point scale, ranging from 1 (No concerned at all to 3 Very concerned). The mean value of all the items are considerable high; starting with concerns over credit card stolen or intercept ( $M = 2.72$ ,  $SD = .455$ ); identity theft ( $M = 2.62$ ,  $SD = .559$ ); physical movement tracking ( $M = 2.55$ ,  $SD = .572$ ); site ask too much personal information ( $M = 2.52$ ,  $SD = .509$ ) and, site share/sell personal information ( $M = 2.52$ ,  $SD = .574$ ). Items which reported to have a low response with 'No concerned at all,' are, a virus could send an email on my behalf (20.7%); email sent may be read by an unknown person (13.3%) and, access to medical report and scam email (10.3%).

**Table 3.** Level of privacy concerns

Items	N	M	SD	No Concerned at all (%)	Somewhat Concerned (%)	Very Concerned (%)
Site not being who they claim they are	29	2.28	.528	3.4	65.5	31
Site asked too much personal information	29	2.52	.509	0	48.3	51.7
Concern over Identity theft	28	2.64	.559	3.6	28.6	67.9
Might access medical records	29	2.28	.649	10.3	51.7	37.9
Unknown people can access my personal information	29	2.59	.628	6.9	27.6	65.5
Credit card details will be intercept/stolen	29	2.72	.455	0	27.6	72.4
Email sent may be read by unknown person	30	2.40	.724	13.3	33.3	53.3
Email sent might be forwarded to other	28	2.39	.629	7.1	46.4	46.4
Received scam email	29	2.28	.649	10.3	51.7	37.9
Legitimate email received may be fraudulent	29	2.45	.572	3.4	48.3	48.3
Computer virus could sent email on my behalf	29	2.31	.806	20.7	27.6	51.7
Site may sell/share my personal information	29	2.52	.574	3.4	41.4	55.2
Site might track my real time movement	29	2.55	.572	3.4	37.9	58.6
Site might track my online purchase	28	2.43	.573	3.6	50	46.4
Site used to gather personal information from outside database/source	29	2.48	.574	3.4	44.8	51.7
Site personalized my preferences based on search history	28	2.39	.497	0	60.7	39.3

**Note:** Measured on 3-point Likert-type item (1 = No concerned at all, 3 = Very concerned)

## 5. Discussion

The study also tries to investigate the perception of researchers towards online privacy. The average age of the respondents ( $M 27.22$ ) showed that this age group is highly privacy perceptive which is in line with the cluster analysis of Kaiser (2016) that showed the average age of 26.84 has the highest privacy perception. This study revealed (76.7%) of respondents believed that online privacy concern also changes with situation and context. This is also

indicated by Bergström(2015), who stated that privacy concerns are a rather contextualized issue. It changes constantly based on the number of uses, awareness and even contradictor. Also, the current study believed their privacy is violated online if data is collected without their consent and that their privacy is violated despite the agreements to sites' privacy policies. In this regard, Youn (2009) pointed out that organizations must strive to provide standardized and regular privacy education to reduce privacy violations. Typically, if privacy policies are adequate and precise, users' can successfully avoid privacy intrusion (Changet al., 2018).

The study showed that more than two-thirds of respondents agree that websites can hinder privacy by collecting their personal information. This is in line with the finding of (Kumaraguru & Sachdeva, 2012), where (71.22%) of the respondents "agree" or "strongly agree" that websites can hinder privacy by collecting personal information. A high score also indicates in ways Internet users' limit the flow of their personal information. Perhaps a report on Americans' lack of confidence over the control of their personal information applies to their communications channels and to the ones who collect their personal information. For instance, (91%) of their survey "agree" or "strongly agree" to users' lost control over their personal information (PEW, 2014). While (43.3%) found it helpful if search engines tracked their search history and used that information to personalize their future search results. It is also equally important as pointed out by (Kaiser, 2016) that the responsibility to mitigate the risks from search engine trackers lies with the search operators.

The present study reported a high level of concerns for credit card and identity theft. Unsolicited intrusions like stealing digital identities (Prince, 2018) are reasonably easy, remarked respondents (Kumaraguru & Sachdeva 2012). From the present study, a high concern for physical movement tracking is also recorded. Similarly, privacy concerns in the study of (Ketelaar & Balen, 2018) revealed negative attitudes towards collecting location data. The current study shows a low level of concern about email, which is the most common attack according to (Chou, 2013; Glasgow & Butler, 2017). For example, when a person submits queries or receives a company response, the person is revealing, and the company is the recipient (Robinson, 2019).

## **6. Limitation and Further studies**

There are some limitations to this study. Firstly, due to the convenience sampling method, the gender ratio is 1:2, with females occupying 63% of the total population. Therefore, the sample was not equally distributed, and this might reduce the generalizability of the results. Therefore, gender differences is not presented in the study. Additionally, the samples from the three departments were not distributed equally (Library Science = 40%; Economics = 43% and Commerce at 17%).

Secondly, since the sample size of the PhD researchers' is limited, future work could include a larger sample size and include various demographic attributes (occupation, state of origin, financial background, educational background, etc.) to represent departments from all schools.

Thirdly, few of the constructs used were not based on validated scales. Maybe incorporating an established or new validated scale to suit the central theme of the future study may allow us to understand the demographic effects on privacy awareness and privacy concerns. Complementing the study with a qualitative approach may also assist in understanding behaviour.



## 7. Conclusion

In this age of clickbait where one is often tempted to click on and explore various internet resources, one becomes vulnerable to the invasion of one's privacy. PhD researchers, owing to their nature of work, tend to wander around the internet regularly in search of information and can compromise their privacy in the process. It is vital that they be aware of the dangers to their privacy and take measures to protect the same. In this regard, the PhD researchers from the Economics, Library Science and Commerce department under the purview of this study seem fairly alert and concerned about their privacy when using the internet. Considering the evolving nature of threats, they need to be consistently alerted and not let their guard down.

## Reference

- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the facebook. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (pp. 36–58). [https://doi.org/10.1007/11957454\\_3](https://doi.org/10.1007/11957454_3)
- Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*, 5, 26–33. <https://doi.org/10.2139/ssrn.889442>
- Aleman, J., del Val, E., Alberola, J., & García-Fornes, A. (2019). Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. *International Journal of Human Computer Studies*, 129, 27–40. <https://doi.org/10.1016/j.ijhcs.2019.03.008>
- Bauer, M., Glenn, T., Monteith, S., Bauer, R., Whybrow, P. C., & Geddes, J. (2017). Ethical perspectives on recommending digital technology for patients with mental illness. *International Journal of Bipolar Disorders*, 5(1). <https://doi.org/10.1186/s40345-017-0073-9>
- Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53, 419–426. <https://doi.org/10.1016/j.chb.2015.07.025>
- Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157–165. <https://doi.org/10.1002/asi.20459>
- Cain, J., & Imre, J. (2021). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media & Society*. <https://doi.org/10.1177/14614448211000327>
- Canares, M. (2018). Online Privacy: Will they Care?, Teenagers Use of Social Media and their Understanding of Privacy Issues in Developing Countries. Retrieved from [https://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport\\_Screen.pdf](https://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport_Screen.pdf)
- Cavoukian, A. (2009). Online Privacy: Make Youth Awareness and Education a Priority. Retrieved June 20, 2020, from <https://www.ipc.on.ca/wp-content/uploads/resources/youthonline.pdf>
- Chang, B. (2021). Student privacy issues in online learning environments. *Distance Education*, 42(1), 55–69. <https://doi.org/10.1080/01587919.2020.1869527>
- Chang, Y., Wong, S. F., Libaqqe-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, 35(3), 445–459. <https://doi.org/10.1016/j.giq.2018.04.002>
- Chen, K., & Rea, J. A. I. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *The Journal of Computer Information Systems*, 44(4), 85–92. <https://doi.org/10.1080/08874417.2004.11647599>

- Chou, T.-S. (2013). Security Threats on Cloud Computing Vulnerabilities. *International Journal of Computer Science & Information Technology*, 5(3), 79–88. <https://doi.org/10.5121/ijcsit.2013.5306>
- Clarke, R. (1999). Internet Privacy Concerns Confirm the Case For Intervention. *Communications of the ACM*, 42(2), 60–67. <https://doi.org/10.1145/293411.293475>
- Culnan, M. J. (1993). “How did they get my name?”: An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly: Management Information Systems*, 17(3), 341–361. <https://doi.org/10.2307/249775>
- De Souza, Z., & Dick, G. N. (2008). Information disclosure on myspace - the what, the why and the implications. *Pastoral Care in Education*, 26(3), 143–157. <https://doi.org/10.1080/02643940802246427>
- Deuker, A. (2010). Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services. In M. Bezzi, P. Duquenoy, S. Fisher-Hubner, M. Hansen, & G. Zhang (Eds.), *IFIP Advances in Information and Communication Technology* (Vol. 320, pp. 275–283). Berlin: Springer. [https://doi.org/10.1007/978-3-642-14282-6\\_23](https://doi.org/10.1007/978-3-642-14282-6_23)
- Dhawan, S., Singh, K., & Goel, S. (2014). Impact of Privacy Attitude, Concern and Awareness on Use of Online Social Networking. In *5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence)* (pp. 14–17). New Delhi: IEEE. <https://doi.org/10.1109/CONFLUENCE.2014.6949226>
- Dinev, & Hart. (2006). Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use. *E-Service Journal*, 4(3), 25. <https://doi.org/10.2979/esj.2006.4.3.25>
- Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295–316. <https://doi.org/10.1057/ejis.2012.23>
- Estabrook, L., Witt, E., & Rainie, L. (2007). Information Searches that Solve Problems: How people use the internet, libraries, and government agencies when they need help. Retrieved from <https://www.pewinternet.org/2007/12/30/information-searches-that-solve-problems/>
- Glasgow, G., & Butler, S. (2017). The value of non-personally identifiable information to consumers of online services: evidence from a discrete choice experiment. *Applied Economics Letters*, 24(6), 392–395. <https://doi.org/10.1080/13504851.2016.1197357>
- Gulliver, A., Bennett, K., Bennett, A., Farrer, L. M., Reynolds, J., & Griffiths, K. (2015). Privacy Issues in the Development of a Virtual Mental Health Clinic for University Students: A Qualitative Study. *JMIR Mental Health*, 2(1). <https://doi.org/10.2196/mental.4294>
- Johns, S., & Lawson, K. G. (2005). University undergraduate students and library - related privacy issues. *Collections and Technical Services*, 47. Retrieved from [http://lib.dr.iastate.edu/libcat\\_pubs/27](http://lib.dr.iastate.edu/libcat_pubs/27)
- Kaiser, A. F. (2016). *Privacy and security perceptions between different age groups while searching online*. University of Twente. Retrieved from <https://essay.utwente.nl/70190/>
- Ketelaar, P. E., & Balen, M. Van. (2018). The smartphone as your follower : The role of smartphone literacy in the relation between privacy concerns , attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, 78, 174–182. <https://doi.org/10.1016/j.chb.2017.09.034>
- Kumaraguru, P., Cranor, L., & Newton, E. (2005). *Privacy perceptions in India and the United States: an interview study*. <https://doi.org/10.1.1.90.6033>
- Kumaraguru, P., & Sachdeva, N. (2012). Privacy in India: Attitudes and Awareness V 2.0. *SSRN Electronic Journal*, 1–51. <https://doi.org/10.2139/ssrn.2188749>
- Lancelot, C., & 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>
- Lee, H., Fan Wong, S., Oh, J., & Chang, Y. (2019). Information privacy concerns and demographic

- characteristics: Data from a Korean media panel survey. *Government Information Quarterly*, 36(2), 294–303. <https://doi.org/10.1016/j.giq.2019.01.002>
- Lee, J., Kwon, S., & Kim, D. (2013). Online Privacy Concerns when Using Online Services (comparison of SNS, cloud storage services, and mobile banking services). In *Recent Advances in Computer Science* (pp. 153–156). WSEAS Press. Retrieved from <https://pdfs.semanticscholar.org/a189/20b6f1829cb2cbe1f1d285f96bfd657e315f.pdf>
- 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>
- Martin, G., Gupta, H., Wingreen, S. C., & Mills, A. M. (2015). An analysis of personal information privacy concerns using Q-methodology. In *ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems*. Cornell University. Retrieved from <https://arxiv.org/abs/1606.03547>
- Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust. *Journal of Business Research*, 82, 103–116. <https://doi.org/10.1016/j.jbusres.2017.08.034>
- Mutambik, I., Almuqrin, A., Liu, Y., Alhossayin, M., & Qintash, F. H. (2021). Gender differentials on information sharing and privacy concerns on social networking sites: Perspectives from users. *Journal of Global Information Management*, 29(3), 236–255. <https://doi.org/10.4018/JGIM.2021050110>
- NEHU. (2021). School of Economics, Management and Information Sciences. Retrieved June 25, 2021, from <https://nehu.ac.in/school/8/School-of-Economics-Management-Information-Sciences>
- Noh, Y. (2020). A study on the changes in librarians' perception before and after user privacy education. *Library and Information Science Research*, 42(3), 101032. <https://doi.org/10.1016/j.lisr.2020.101032>
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). New York: McGraw-Hill. <http://vlib.kmu.ac.ir/kmu/handle/kmu/84743>
- Ozeran, L., Solomonides, A., & Schreiber, R. (2021). Privacy versus Convenience: A Historical Perspective, Analysis of Risks, and an Informatics Call to Action. *Applied Clinical Informatics*, 12(2), 274–284. <https://doi.org/10.1055/s-0041-1727197>
- Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of "privacy concerns" and "privacy actions." *International Journal of Human Computer Studies*, 65(6), 526–536. <https://doi.org/10.1016/j.ijhcs.2006.12.001>
- PEW. (2014). Public Perceptions of Privacy and Security in the Post-Snowden Era. Retrieved June 27, 2021, from <https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/>
- Prince, C. (2018). Do consumers want to control their personal data? Empirical evidence. *International Journal of Human-Computer Studies*, 110, 21–32. <https://doi.org/10.1016/j.ijhcs.2017.10.003>
- Robinson, S. C. (2019). No exchange, same pain, no gain: Risk–reward of wearable healthcare disclosure of health personally identifiable information for enhanced pain treatment. *Health Informatics Journal*, 25(4), 1675–1691. <https://doi.org/10.1177/1460458218796634>
- Rogers, E. M. (1983). *Diffusion of innovations*. The Free Press (3rd ed.). The Free Press.
- Sheehan, K. B. (2002). Toward a typology of internet users and online privacy concerns. *Information Society*, 18(1), 21–32. <https://doi.org/10.1080/01972240252818207>
- Shepherd, R. P. (2016). Men, women, and Web 2.0 writing: Gender difference in Facebook composing. *Computers and Composition*, 39, 14–26. <https://doi.org/10.1016/j.compcom.2015.11.002>
- Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. *Computers in Human Behavior*, 54, 114–123. <https://doi.org/10.1016/j.chb.2015.07.062>
- Tavani, H. T. (1999). Informational privacy, data mining, and the Internet. *Ethics and Information Technology*,

I(2), 137–145. <https://doi.org/10.1023/A:1010063528863>

TRUSTe LLC. (2004). Online Privacy Questionnaire. Retrieved December 20, 2020, from [https://www.cc.gatech.edu/gvu/user\\_surveys/survey-1998-04/questions/privacy.html](https://www.cc.gatech.edu/gvu/user_surveys/survey-1998-04/questions/privacy.html)

Tuunainen, V. K., Pitkänen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites - Case Facebook. In *22nd BLED eConference eEnablement: Facilitating an Open, Effective and Representative eSociety - Proceedings* (pp. 1–17). Retrieved from <https://www.semanticscholar.org/paper/Users%27-Awareness-of-Privacy-on-Online-Social-Sites-Tuunainen-Pitkänen/9b833ca55abd01f842c764804706750743c67115>

Warren, S., & Brandeis, L. (1890). The Right to Privacy. In *Harvard Law Review*. Retrieved from [https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy\\_brand\\_warr2.html](https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html)

Westin, A. F. (1969). Privacy and Freedom. *Administrative Law Review*, 22(1), 101–106. Retrieved from <https://www.jstor.org/stable/40708684>

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents. *Journal of Consumer Affairs*, 43(3), 389–418. <https://doi.org/10.1111/j.1745-6606.2009.01146.x>

\*\*\*\*\*