Factors Affecting Data-Privacy Protection and Promotion of Safe Digital Usage

Rituparna Chakraborty [1], G S Prakasha [1] and C K Sripavithra [1, 2]

[1] *Christ University, Central Campus, Bangalore, 560029, India*
[2] *Maharani's Science College for Women, Mysore, 570005, India*

Abstract

India is facing the problem of the digital divide. Being developing countries and with low literacy rates, digital knowledge among the public is weak. Those who know a bit about digital operations on smartphones and computers are not having complete knowledge of data security and its peculiarities. Therefore, this study aimed to find determinants of data-privacy anxiety among Indians and to understand their stress and anxiety during the use of digital applications in their daily routines, especially amid the COVID-19 scenario. The current study adopted an inductive qualitative exploratory approach to delve into the above issues. This study employed a reflexive thematic analysis method to analyse interview data of 10 participants across young-adult to middle-adult age groups of male and female gender. Participants belonged to middle socio-economic status having urban background. The study found 6 themes and 26 sub-ordinate themes as determinants of data-privacy anxiety. Emerging themes from the data indicated at the systemic determinants of data-security anxiety, the paradox of learned helplessness and convenience preference among participants. This paper employed the Foucauldian lens of bio-power to discuss the circumscribing function of ill-structured knowledge dissemination approaches. This paper argues in favor of a critical pedagogy approach in educating people about digital security, dealing with data-privacy anxiety, and promoting safe digital usage among all generations of Indians. It also suggests measures of modifications in policies and documentation processes of major online platforms and apps to curb uncertainty and sense of insecurity among users.

Keywords

Anxiety, Data-security, Data breach, Online Apps

1. Introduction

India is a developing country with a 77.7 % literacy rate. 40% of the population live below the poverty line. Digital literacy is almost non-existent in India. However, with the advancement in technology across the globe people are forced to use digital platforms for their various purposes in daily life. According to a 2016-17 survey, India is the second country in the world, after China, in the number of internet users. India has 391 million people using the internet daily [1]. India has several digital platforms for the public under the flagship programme called Digital India. Social awareness is an important factor for internet transactions [2]. Recently smartphones became easily available to common people all over India and private companies are providing internet services at cheaper prices. Therefore, the public is using digital platforms without much knowledge of their usage and the conditions laid out by app developers. Smartphone users have significant concerns over data breach [3]. Studies indicate that activity patterns like not locking screens of smartphones are indicative of a lack of awareness about

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia
EMAIL: rituparna.chakraborty@christuniversity.in (Rituparna Chakraborty), prakasha.gs@christuniversity.in (G S Prakasha), sripavithra.ck@res.christuniversity.in (C K Sripavithra).
ORCID: 0000-0001-6023-3728 (Rituparna Chakraborty), 0000-0002-1287-7606 (G S Prakasha), 0000-0003-4325-4564 (C K Sripavithra).

possible risk and data-breach [4]. Consequently, there is a rampant breach of data security.[5] There is a surplus amount of data stealing and misuse across India and many parts of the world.

India is a country with the highest youth population, housing almost 500 million people studying and working. Many of them are the victims of cyberbullying. Cyber-bullying has been established as a predictor of loneliness in the young population of multiple countries.[6] They use online apps for almost every daily routine such as ordering food, clothing, entertainment, shopping, bill payments, etc. Recently there is a rise in the number of cases of data theft and SMS alerts are being sent by various authorities on non-disclosure of personal information. Owing to this, people have anxiety and stress on data insecurity while every online transaction they do. Research studies have shown that significant portions of consumers have privacy concerns related to online shopping [7]. Academic studies have already argued that security-related stress has not been given due importance in information systems research.[8] There is a need for a well-defined role of individuals towards internet anxiety [9].

In the 2000s, a new psychological term was coined, related to the anxiety created by online health-information search. The print media of the UK first coined the term 'cyberchondria'. This term became more relevant during the COVID-19 pandemic of 2020. Rise in the rampant search of health-related information during this time made it more relevant. Such information search was done with or without checking the authenticity of source websites. After some time, it was also seen that such anxiety reinforced anxiety related to data privacy, plausibly resulting from an unbridled search.

During the pandemic in 2020, the whole world shifted to online for personal and professional requirements. On one hand, this led to progress in digital literacy, on the other; it also created the need for educating people about cyber-security. In 2020 alone, officially more than 40 large-scale conferences have happened in India on cyber-security [10]. Other than this, numerous institutional level programs have happened on the same. Such information dissemination, although necessary, also can lead to significant anxiety about data security. Previous research indicated a possible solution to such anxiety through a balanced information search [11]. Using a Foucauldian concept of Bio-power, the role of 'knowledge' can be scrutinized in this case for a contextual understanding of such anxiety.

Recently, in the beginning of 2021, the world saw one of the largest digital exodus related to the messaging application Whatsapp. India was also among the frontrunners. Multiple sources have already accepted that the majority of people consider Google and Facebook to be primary encroachers of data privacy.[12] Their advertisement feeding process is dependent on collecting personal information and digital-activity patterns of individuals. The pervasiveness of data-security stress has already been indicated by scholars, related to personal-identifiers of different sectors [13, 14]. Such anxiety becomes graver when it comes to personal communications. Whatsapp was overtaken by Facebook a few years back. People started migrating to other messaging apps due to Whatsapp's announcement of a data-sharing agreement with Facebook. In a span of 72 hours, other messaging apps like Telegram or Signal observed an almost 500% increase in new users [15]. Such incidents and review of previous research indicate the necessity to delve into the pattern and determinants of data-privacy anxiety among people and the possible ways of dealing with it [16] [17].

Overview of the literature showed that data-security has been mostly researched in the field of computer application and electronics, where most emphasis has been on the processes. In behavioral sciences there has been a dearth of work on this topic. Few studies which have talked about the effects of data-security breach limited the work within suggestions of campaigns to increase awareness among people. There is almost no work evaluating the effects of such programs or delving into the pedagogical need. The psychological anxiety due to data-breach is talked about in very few studies, in the last few years, but those works are mostly limited to health-information search, evidently not expanding to everyday usage of the internet in all aspects of our lives. Literature review also indicated the imminent necessity of such psychological and educational approach to study this indispensable part of media.

2. Research Question

Present study aimed to find the determinants of data-privacy anxiety among the Indian public in the age group of 20 to 40 through qualitative research design.

Incidentally, study framed the following sub-research questions,

- Whether the use of a mobile-banking facility is influenced by anxiety about data breaches.

- Does the pattern of health-information search during the pandemic show any influence of privacy policies of accessed websites?
- Are we comfortable using online apps for daily routines?
- Is the use of pay apps for various purchases a threat to bank account data?
- Use of Medical apps or fitness apps amid COVID-19 and the possibility of data leakage.
- How do we reduce overthinking on data security?
- Is Social media blowing up data breaches alarmingly?
- Hacking Is Alarming. So are Data Brokers?
- Are information security policies raising the anxiety of people by invading privacy?

3. Methods

This paper followed a qualitative exploratory research design. Through open-ended semi-structured interviews for data collection, this study delved into the contextual determinants of data-privacy anxiety. 10 participants from young-adult to middle-adult age group 20-40 were interviewed for this study. Participants belonged to middle socio-economic status and urban background. The interviews were audio-recorded following APA ethical guidelines for the same. Interviews were conducted in English and were not translated for analysis. Braun & Clarke's [55] method of reflexive thematic analysis was followed for analyzing the data. The research adopted a social-constructivist epistemological lenses for data analysis. The article has acknowledged the authors, whose work have been built upon conceptually, through in-text citations and full reference in the reference section. Table 1 and 2 below presents the interview guide used for the study and the demographic details of the participants.

Table 1.
Interview Guide

- Can you share your experience of using online platforms? (Probe: what are the apps they use? Which apps they are comfortable with)
- Which apps do you use for your daily needs? Which features make you comfortable using them?
- How many apps do you use that include financial exchange? Are you comfortable using them? What makes you feel this way? (Probe: pros & cons)
- How was your experience of using online platforms post COVID-19 breakout? (Probe: which purposes they use it & are comfortable with it)
- Are there any challenges or concerns in using online platforms? What are those?
- Do you possess knowledge about data security? How do you know about it? (Probe: whether it is organised programme like seminars or random unofficial/official news or messages)
- Does this knowledge help you in any way? (probe: if yes/no how and why; any modifications in online behavior after that)

Table 2.
Demographic details of the participants

Pseudonym	Gender	Age	SES	Locality
P1	M	38	Middle	Urban
P2	M	35	Middle	Urban
P3	F	25	Middle	Urban
P4	M	21	Middle	Urban
P5	F	31	Middle	Urban
P6	F	28	Middle	Urban
P7	M	26	Middle	Urban
P8	F	32	Middle	Urban

Pseudonym	Gender	Age	SES	Locality
P9	M	22	Middle	Urban
P10	F	30	Middle	Urban

4. Results and Discussion

Academic research indicated the need for balanced-research in reduction of anxiety related to data-hacking among people.[11] Most of the academic research on this field focused on population from developed countries. However, India has approximately 400 million internet users.[1] Literacy rate in India is around 75%, however digital literacy is way lesser.[18] Scholars have indicated that how users interpret security measures on online platforms can influence their related sense of assurance or anxiety.[19] It can be argued that lack of digital literacy is one of the main determinants of internet-anxiety. Digitally illiterate or partially literate sections of the population may fall prey to data-hacking more commonly. Consequently, such experiences may reinforce internet-anxiety among this population.

Emerging themes from analysis of data were primarily connected to the anxiety igniting the possible debate of utilitarian value of digital medium versus security or safety approach. Major themes that emerged from the data and the converging sub themes have been presented in Table 3. In total, there are 6 main themes and 26 subordinate themes as revealed by the thematic analysis.

Table 3.
The emerging themes and subthemes from the analysis of data

Themes	Sub Themes
Convenience a utilitarian approach	• Preference for convenience over privacy • Comfort with instant solution of needs • Majority of need satisfaction • Life-boat during pandemic restrictions
Perception of control	• Usage of data-privacy features in app • Customized settings in most applications • Less frequent conflict of data breach • Promises of data-encryption by digital app
Anxiety and learned helplessness	• Dependency on digital platforms • Government mandates • Lifestyle modifications • Anxiety over high-stake information • Reports of digital vigilance and data leakage • Frequency of cross platform customized advertisements • Knowledge about governmental reach of information • Difficulty in meaning-making for digital-migrants
Compensatory mechanism for anxiety	• Usage of safe-mode internet search • Limiting data-sharing • Avoidance of using unnecessary platforms • Frequent change of passwords

Themes	Sub Themes
Data-security - an oxymoron	• Inability of abandoning usage of digital platforms • Permanence of digital footprint • Mutual exclusiveness of data privacy and seamless usage
Circumscribing function of knowledge	• Too much information creating anxiety and panic • Information increasing habit of generalization • Information creating conflict, self-blame and guilt

It was seen mostly in the responses of middle adult participants, that the nature of complicated and ambiguous usage of English language in most applications create a sense of anxiety in them. This generation of people are mostly digital-migrants, who are not acquainted with many digital terms and their appropriate applicatory meanings. In line with these, another factor that should be discussed is the use of the English language primarily in most data-privacy statements. Although multiple online websites and applications provide the options of using regional language for communication. These have started after the digital India movement of the Indian government. Primary intentions behind such policies were to facilitate internet use among maximum Indians, who may not be comfortable with the English language. The majority of regional language facilities are provided for search engines and messaging facilities, whereas the processes of making accounts in those websites follow the English language primarily. Similar trends are seen in social-media platforms. This paper argues this to be a possible factor influencing anxiety related to breach of data-privacy. To make accounts in any of the popular or most used websites and applications, users are required to accept privacy statements and agreements. The length of such agreement policies and invariable use of English language leads to blind acceptance of such policies among a significant section of Indian population. Consequently, this leads to underlying apprehension and anxiety about data-privacy, as most users are not fully aware of details of the policies. This paper proposes a possible solution of reducing such data-privacy anxiety through dealing with the contextual determinant of language barrier. Online platforms should mandatorily provide options of reading privacy agreements in regional languages, to make it completely legible for users. Additionally, they should also focus on content organization of privacy agreements. Such agreements should consist of a short content with highlighted relevant points on privacy protection and avoid technical jargons to accommodate digital-migrants.

As reflected in news reports, online giants like - Google or Facebook are considered by many Indians as privacy-invaders.[12] Major determinant of such perception is based on the personalization of advertisements shown in individual's accounts and webpages. The data of the current study also showed a similar pattern, where participants across age-groups reported increased anxiety caused by customized advertisements in other digital platforms, based on their usage of one platform. Similar concerns were argued by Laluandala in his systematic review of Facebook data-breach.[20] The personalized nature of advertisements make it evident that personal information and digital-activity patterns of individuals are not only recorded in the websites, but also shared with marketing agencies. The recent 2021 digital exodus from messaging app Whatsapp was a reflection of such data-privacy anxiety. As reflected in participants' opinions, social media platforms like Facebook provide free gaming options, which are mostly dependent on data-sharing processes. The primary data collected by the social media website or application is also shared with the gaming website or application, which follows considerably lower levels of data-privacy measures. This paper argues that such data-sharing agreements between online platforms are a significant source of data-leakage and this issue becomes more profound due to the fact that the majority of users in these platforms are young people, making impulsive choices about those gaming options.

This paper points out with the help of emerging themes from the data, that anxiety or tendency to overthink about data security may even increase while using paying applications of such companies. According to a 2019 survey google pay is one of the most used paying applications in India, with 59% of Indians using it [21]. In the present study, almost 100% of users informed about using the same

paying application. Such paying applications ask for online banking passcode and access to all phone contacts during initial creation of the account. Such compliance activities in online platforms have been identified as a source of consumer anxiety [17]. This paper argues that lack of trust in the owner company and the processes of initiation work are determining factors in creating anxiety while using such applications. Previous research also points out the role of individual perception and belief to be moderating factors of data-privacy anxiety [9]. Additionally, the learned helplessness arising from obligatory and habitual usage of financial exchange applications function as contributory factors in the increment of anxiety, as reflected in participants' opinion of this study. Online platforms need to work on building trust about data safety among users. During the pandemic, multiple sections of society were obligated to use online modes of payments for daily needs. This was primarily due to the fear of contamination through physical currency exchange. Such circumstances created a ground of overarching anxiety related to data-privacy and simultaneous sense of learned-helplessness. Scholars have indicated the necessity of focussing on autonomy and subjective rights of users in order to reduce security anxiety.[22][23][24] Current paper argues for a change in such data-privacy processes, in terms of providing options of alternative ways of connecting paying applications to bank accounts, bypassing banking password entries or phone contact access. Data-sharing agreements between social-media platforms and related gaming or entertainment applications need to be modified as well to curb data-breach. Such modifications may reduce convenience, although might subsequently reduce data-privacy anxiety.

Similar scenarios can be observed in relation to online shopping applications - like amazon, big basket or flipkart. Previous studies indicated the frequency of online shopping among the young population in India [25]. However, the pandemic and subsequent lockdown changed the online shopping scenario. From convenience-based it turned into necessity-based shopping. The participants of the current study clearly indicated their preference towards convenience in comparison to data privacy, although the knowledge of the same is a frequent source of anxiety regarding data-leakage. Recently Google officially declared top 5 search trends in India during 2020 and it was evident from that report that Indians are moving online for their daily basic requirements, from food to medical assistance [26]. Consequently there was an expansion of online buyers' age-group and usage of a variety of applications. Participants also expressed the reality of their habitual modification of lifestyle which has made the cessation of digital usage impossible. It was also seen that participants adopt compensatory mechanisms to deal with such anxiety, mostly focusing on some sort of control over data-sharing. Majority of financial exchange applications have taken a few additional convenient measures like QR-code usage, although scholars indicated those measures also contributing to consumers' data-security anxiety [27]. It is an established fact that the more people use the online search engines, the more anxious they are about data-privacy [28].

Research on social media networks reveals that information collection patterns of these platforms create anxiety about privacy and data-security among users [29]. These apps also have personalized product advertisements, based on previous search patterns. This creates an underlying perception of lack of agency and subsequent anxiety related to data-security. These shopping applications also add payment methods and chosen options as default. If users are unaware or lack literacy regarding changing the options, data-hacking and cyber-crime possibilities increase. The data of the current study clearly showed a trend of this anxiety across age-groups of participants, where middle-aged participants expressed higher amounts of worry and anxiety over data-leakage. Previous research indicated that online platforms need to become more transparent about their intentions in order to decrease user anxiety.[30][31][32] They also argue the importance of perception of intent over digital-security advice, where mere listed advice do not function well without required transparency on the same.[33][34] This paper argues that there is a strong need for change in such policies to increase assurance and decrease anxiety among users. Online shopping applications need to focus on securing financial information of individuals, thereby not opting for default payment options.

As discussed previously, internet search for health-related information and subsequent anxiety became prevalent since the outbreak of pandemic. This led to the coining of the term 'cyberchondria'. Studies on health-information search trends indicate that trust of users depends on credibility of the website and convenience of use [35]. This paper argues that logically these two factors may be opposing each other at times. Participants of the current study also articulated this paradox, indicating the obligatory usage of multiple digital platforms and apparent lack of control over data-sharing, along with

illusory perception of control over the same. Indian media promoted government directives and websites for health-related information during pandemic. US based studies previously showed that users might become anxious about data security with perceptions of government-surveillance [36]. One participant of the current study also mentioned about an incident where an apparently "permanently" deleted message in a messaging application, surfaced up during a government mandated data-surveillance by her government-employee family member. Participants articulated frequently about the permanence of digital-footprint in such contexts, which is a strong determinant of learned-helplessness and anxiety related to data-security. They also indicated how health-related information searches were one of the primary sources of their anxiety during the pandemic. Indian government websites are mostly less easy to access in comparison to private search-engines and websites, which provide direct short answers. Empirical studies also have shown that limited knowledge of users make them vulnerable to online frauds frequently.[37] Mentioned scenario of accessibility coupled with limited digital literacy in India is a possible determining factor for data-leakage and subsequent reinforcement of internet-anxiety. In this context this paper argues, being in-line with the emerging themes, that digital security in India is almost an oxymoron, where the permanency of digital footprint and accessibility of data by authorities make it pragmatically impossible to have any privacy once an individual enrolls into the digital world.

Educating internet users about possible data-breach and required safety-measures is one of the primary necessities of the moment. Academic research has indicated both positive and negative roles of technical knowledge in reducing data privacy anxiety [38], [39], [40], [41]. Such research studies also talk about the importance of mental health of people related to data-privacy anxiety [42], [43]. As mentioned above multiple government and private initiatives on such fronts have been witnessed in recent times.[10] Previous studies talked about the effects of such information dissemination on the online company trades, but effects on consumers have rarely been discussed [44], [45]. However, it can also be argued that over-information on topics of privacy can influence subsequent anxiety in users. Most of the formal institutional awareness initiatives in contemporary society highlight all possible methods of data-hacking and privacy-breach. Requirement of a social constructivist approach in studies of data-privacy anxiety has been advocated before [46]. Current study used such approach to analyses the systemic determinants of anxiety rooted in the authoritative structure of knowledge dissemination. Participants of the present study indicated the circumscribing role of such knowledge acquisition, in comparison to the empowering function. Majority (80%) of these participants spoke about the increased anxiety and panic that they faced after acquiring such knowledge from multiple formal and informal sources. They also articulated regarding increment in compensatory activities to deal with such arising anxiety, and the resultant helplessness and hopelessness through realization of its futility. Research studies highlighting experiential accounts of employees related to technological fields hint at the downside of over and continuous information related to data-breach and security measures.[47] Current paper uses Foucauldian lens of biopower, to argue that such abundant 'knowledge' can work even in the way of circumscribing online movement of every individual, making them paranoid about possible privacy-invasion. Individuals are continuously thinking about possible ways of data-breach, which in its own way creates anxiety. With limited technical and digital knowledge, individuals may develop a sense of inadequacy related to protection from surveillance and data-hacking. This issue becomes more profound when discussed related to mobile-internet. Scholars pointed out the increasing data-breach and related anxiety in use of mobile-internet [48]. Yu indicated gender and age to be moderating factors for usage of mobile-banking, along with credibility of medium [49]. The current sample of participants also showed similar trends of differential belief in competence and mastery over mobile-internet usage among male and female participants and young-adult and middle-adult participants. Previous research shows the importance of users' trust on the platform in mobile-banking segments [50]. Majority of older generations' people in India don't feel comfortable using online-banking due to their limited technical and digital knowledge, which corroborates the digital-migrant participants' accounts in the current study. Scholars already pointed out the legal difficulties of dealing with data-breach issues [51]. Limited technical knowledge and age may be additional factors in such circumstances. Uncertain circumstances of the current pandemic-stricken world and compelling need to depend on online mediums for daily requirements have significantly added to it. Previous studies indicated the necessity for a user-involving approach [52]. This paper argues that a critical pedagogy approach needs to be adopted for conducting programs on data-safety. Such programs should be customized depending on the social-locations of

audiences. There is ample evidence that data-privacy concerns are different for different age-groups and sections of people.[19] Such inclusive pedagogical approach can work as a possible solution to curb anxiety caused by abundance of information dissemination. Simultaneously such initiatives will also promote safe usage of online facilities among all age groups from all parts of India.

5. Conclusion and suggestions for further studies

Data-privacy anxiety is only a beginning for a country like India, which has been accentuated by the obligatory usage of digital platforms in contemporary pandemic scenarios. As people gradually become aware of the data-thefts and cyber crimes happening around the world, the data-privacy anxiety will further increase in size. This current study argues an imminent necessity for critical pedagogical approaches in offering cyber-awareness programs. There is a need to move towards accessible functional approaches instead of following traditional knowledge dissemination methods. The paper additionally argues in favor of transparent people-friendly policies to ensure data-security and decrease anxiety among internet-users. There is a need to consider contextual parameters and limitations of probable users while drafting the policies. This current paper also advocates a necessity to study such indispensable and complicated parts of media from a multidisciplinary approach. Drafts of digital applications need to incorporate educational methodologies and psychological insights into their process.

The present paper urges the future researchers to delve deep into this topic with more quantitative and qualitative research. Qualitative research may focus on the users' behavior and psychological determinants behind usage of online applications and quantitative research may focus on developing people-friendly policies and foolproof methods for application developers.

6. Conflict of Interest

There is no conflict of interest among the authors. All authors have equally contributed to the paper.

7. References

[1] https://ourworldindata.org/internet Accessed January 2021.

[2] Dinev, T., & Hart, P. Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce (2005). 10(2), 7-29.

[3] Mamonov, S., & Benbunan-Fich, R. An empirical investigation of privacy breach perceptions among smartphone application users. Computers in Human Behavior. (2015), 49, 427-436.

[4] Albayram, Y., Khan, M. M. H., Jensen, T., & Nguyen, N. "... better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In Thirteenth Symposium on Usable Privacy and Security {SOUPS} (2017) (pp. 49-63).

[5] Stanislav Mamonov, Raquel Benbunan-Fich. An empirical investigation of privacy breach perceptions among smartphone application users, Computers in Human Behavior. (2015)

[6] Al Qudah MF, Al-Barashdi HS, Hassan EMAH, Albursan IS, Heilat MQ, Bakhiet SFA, Al-Khadher MA. Psychological Security, Psychological Loneliness, and Age as the Predictors of Cyber-Bullying Among University Students. Community Ment Health J. Apr (2020). 56(3):393-403. doi: 10.1007/s10597-019-00455-z. Epub 2019 Sep 14. PMID: 31522350.

[7] Miyazaki, A. D., & Fernandez, A. Consumer perceptions of privacy and security risks for online shopping. Journal of Consumer affairs. (2001), 35(1), 27-44.

[8] Ament, C., and Haag, S. "Security-Related Stress: A Neglected Construct in Information Systems Stress Literature," in Proceedings of the 24th European Conference on Information Systems (ECIS 2016), Istanbul, Turkey (2016).

[9] Thatcher, J. B., Loughry, M. L., Lim, J., & McKnight, D. H. Internet anxiety: An empirical study of the effects of personality, beliefs, and social support. Information & Management. (2007), 44(4), 353-363.

[10] Dalziel, H. Cyber Security Conferences and Events in India. (2020) https://infosec-conferences.com/country/india/
[11] Valentino, N. A., Banks, A. J., Hutchings, V. L., & Davis, A. K. Selective exposure in the Internet age: The interaction between anxiety and information utility. Political Psychology. (2009), 30(4), 591-613.
[12] Aravind, V. The great WhatsApp migration of 2021: How India is waking up to privacy issues. (2021)
[13] https://www.newslaundry.com/2021/01/16/the-great-whatsapp-migration-of-2021-how-india-is-waking-up-to-privacy-issues
[14] Jasmine Henry. 9 Reasons Why Cybersecurity Stress Is an Industry Epidemic. (2020)
[15] Smith, T. T. Examining data privacy breaches in healthcare. (2016)
[16] Cuthbertson, A. Whatsapp Privacy Controversy Causes 'Largest Digital Migration in Human History', Telegram Boss Says As He Welcomes World Leaders. (2021) https://www.independent.co.uk/life-style/gadgets-and-tech/whatsapp-privacy-telegram-world-leaders-b1787218.html
[17] Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. Consumer attitudes toward data breach notifications and loss of personal information. Rand Corporation. (2016)
[18] Kim, K., Kim, B., & Koo, Y. Effect of the Justice of Personal Data Breach Notification and Perceived Security Level on Individual Psychological Responses: A Multi-theoretic Approach. The Journal of Internet Electronic Commerce Research (2019), 19(4), 59–79.
[19] Rajput, A., & Nair, K. Significance of digital literacy in e-governance. The SIJ transactions on industrial financial & business management (2013), 1(4).
[20] Lundgren, M., & Bergström, E. Security-related stress: A perspective on information security risk management. International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (June 2019) (pp. 1-8). IEEE.
[21] Lulandala, E. E. Facebook Data Breach: A Systematic Review of Its Consequences on Consumers' Behaviour Towards Advertising. Strategic System Assurance and Business Analytics (2020), 45-68.
[22] https://www.statista.com/statistics/1034443/india-upi-usage-by-platform/
[23] Cohen, J. E. Examined lives: Informational privacy and the subject as object. Stan. L. Rev. (1999), 52, 1373.
[24] Cohen, J. E. What privacy is for. Harv. L. Rev. (2012), 126, 1904.
[25] Inglehart, R. F. The danger of deconsolidation: How much should we worry?. Journal of Democracy (2016), 27(3), 18-23.
[26] Vaidya, A., & Vaidya, V. Online shopping trends among college students. International Journal of English language literature in humanities. (2017)
[27] https://bestmediainfo.com/2020/05/google-india-reveals-top-5-emerging-trends-in-online-searches-and-insights-for-brands/ Accessed January 2021.
[28] Okazaki, S., Navarro-Bailón, M. Á., & Molina-Castillo, F. J. Privacy concerns in quick response code mobile promotion: The role of social anxiety and situational involvement. International Journal of Electronic Commerce (2012), 16(4), 91-120.
[29] Banerjee, S. How Does the World Google the Internet, Anxiety, and Happiness?. Cyberpsychology, Behavior, and Social Networking, (2018) 21(9), 569-574.
[30] Osatuyi, B. Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. Computers in Human Behavior (2015), 49, 324-332.
[31] Johnston, A.C. and Warkentin, M. "Fear Appeals and Information Security Behaviors: An Empirical Study", MIS Quarterly (2010), (34:3), pp. 549–566.
[32] Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. Transparency of intentions decreases privacy concerns in ubiquitous surveillance. Cyberpsychology, Behavior, and Social Networking (2014), 17(10), 633-638.
[33] Hoehle, H., Aloysius, J.A., Goodarzi, S., and Venkatesh, V. "A nomological network of customers' privacy perceptions: Linking artifact design to shopping efficiency," European Journal of Information Systems (2019), (28:1), 91-113.

[34] Rhee, H.-S., Kim, C., & Ryu, Y. U. Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security (2009), 28(8), 816–826.
[35] Redmiles, E. M., Malone, A. R., & Mazurek, M. L. I think they're trying to tell me something: Advice sources and selection for digital security. In 2016 IEEE Symposium on Security and Privacy (SP) (May 2016) (pp. 272-288). IEEE.
[36] Corritore, C. L., Wiedenbeck, S., Kracher, B., & Marble, R. P. Online trust and health information websites. International Journal of Technology and Human Interaction (IJTHI) (2012), 8(4), 92-115.
[37] Dinev, T., Hart, P., & Mullen, M. R. Internet privacy concerns and beliefs about government surveillance–An empirical investigation. The Journal of Strategic Information Systems (2008), 17(3), 214-233.
[38] Grazioli, S., & Jarvenpaa, S. L. Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans (2000), 30(4), 395-410.
[39] Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. "My Data Just Goes Everywhere:" User mental models of the internet and implications for privacy and security. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)(pp. 39-52).
[40] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. Information security conscious care behaviour formation in organizations. Computers & Security (2015), 53, 65-78.
[41] Elhai, J. D., & Hall, B. J. Anxiety about internet hacking: Results from a community sample. Computers in human behavior (2016), 54, 180-185.
[42] Elhai, J. D., Levine, J. C., & Hall, B. J. Anxiety about electronic data hacking. Internet Research. (2017)
[43] Elhai, J. D., & Frueh, B. C. Security of electronic mental health communication and record-keeping in the digital age. The Journal of clinical psychiatry (2016), 77(2), 262-268.
[44] Juta Gurinaviciute. Mental health warning in cybersecurity: CISOs across the industry reporting high levels of stress. (2020) https://www.securitymagazine.com/articles/93710-mental-health-warning-in-cybersecurity-cisos-across-the-industry-reporting-high-levels-of-stress Accessed January 2021.
[45] Cavusoglu, H., Mishra, B., & Raghunathan, S. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, (2004) 9(1), 70-104.
[46] Martin, K. D., Borah, A., & Palmatier, R. W. Data privacy: Effects on customer and firm performance. Journal of Marketing (2017), 81(1), 36-58.
[47] Malhotra, N. K., Kim, S. S., & Agarwal, J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research (2004), 15(4), 336-355.
[48] Ty Sbano, Advanced persistent stress: Why security pros need rituals.
[49] https://techbeacon.com/security/advanced-persistent-stress-why-security-pros-need-rituals. Accessed January 2021.
[50] Thompson, N., McGill, T. J., & Wang, X. "Security begins at home": Determinants of home computer and mobile device security behavior. Computers and Security (2017), 70, 376–391. https://doi.org/10.1016/j.cose.2017.07.003
[51] Yu, C. S. Factors affecting individuals to adopt mobile banking: Empirical evidence from the UTAUT model. Journal of electronic commerce research (2012), 13(2), 104.
[52] Ouyang, Y. A use intention survey of mobile banking with smart phones-an integrated study of security anxiety, Internet trust and TAM. Innovative Marketing (2012), 8(1), 15-20.
[53] Solove, D. J., & Citron, D. K. Risk and anxiety: A theory of data-breach harms. Tex. L. Rev (2017), 96, 737.
[54] Albrechtsen, E. "A Qualitative Study of Users' View on Information Security," Computers & Security. (26:4), (2007) pp. 276–289.
[55] Braun, V. & Clarke. V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101