A study on privacy concerns across social networking sites: An Indian perspective

RAVNEET SINGH BHANDARI
SANJEEV BANSAL

Abstract

Various past studies on online privacy have described different aspects of users' privacy concerns. The objective behind this paper is to build up empirical evidence between existing theories with subsequent reactions from users utilising social networking sites. An online survey of 352 social networking users was conducted whereby respondents were asked to respond on identified variables of privacy while utilising social networking sites. The outcomes show that effective notification, securitisation and legalisation of privacy policies have a positive impact on privacy concerns. More interestingly, the results demonstrate that an apparent absence of legitimate approach or legislative direction would result in users' endeavour to withdraw their respective data from the social networking site.

To understand user privacy concerns and for better results, researchers need to give more consideration to the website privacy control mechanisms and judiciary systems worldwide emphasising on creating prominent self-controls. Website regulators can enhance user privacy by additionally characterising and enhancing the legitimate system for ensuring user protection on the web. This paper attempts to understand the existing privacy structure on social networking sites and impact of these control measures on user online privacy concerns.

Keywords: *Online privacy, Social networking sites, Government of India, Privacy concern*

Introduction

The constantly increasing usage of the internet and the database of Individual Identifiable Information (I3) has been raising serious privacy concerns over the past few decades. To be specific, there are concerns about how database holders of Individual Identifiable Information (I3) collect data over various online platforms. This process primarily involves three players: developers, government, and users (Stewart & Segars, 2002). Developers across various online platforms, at present, are facing rough pronouncements while creating their privacy strategies and policies (Rosen, 2001). These informational databases can be lucrative for online site administrators as they can commercially transfer it to third parties i.e. marketers, in order to improve their respective product offerings and services (Charters, 2002). Additionally, numerous third parties are involved in collecting, analysing, interpretation and commercialising individual information (Lowry, Cao, & Everard, 2011). Perhaps, gathering and storing users' personal information on social networking sites also includes substantial risk, as evidenced in case of Cambridge Analytica using social media profile data for political campaigning (Dasgupta, 2018).

Data violations scams are growing at an alarming rate and the impact on social relations and financial fallout from such violations are enormous. Site administrators must review the implications of these risk propositions while they formulate their privacy code of conduct (Hong & Thong, 2013). In a review of high profile data violation cases, judiciary and government—the next significant player—have defined two aspects of privacy violations: (1) holding site administrators liable for any data violation, levying penalties, and even de-licensing those that handle user data illegitimately and (2) enhancing the level of privacy, providing formal standards for data migration to promote storing practices (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). The policy makers, however, must persistently review the current state of public privacy policies across social networking sites and revaluate the structure of the policies established whenever required (Bryce & Klang, 2009). The last significant player is the users, based on three outlines of usage (1) how they are informed about the privacy system of the site (2) to enhance the privacy of the user, whether they are served with selective options and (3) if required, modifications in the privacy settings are available or not (Rathore, Ilavarasan, & Dwivedi, 2016).

Information privacy policy in India

In India, Information Technology Act (ITA) 2000 administrates information privacy issues. This act offers guiding principles for individual online privacy protection (Sumanjeet, 2002). The procedures are based on a resolution passed on 30th January, 1997 i.e. Model Law on Electronic Commerce and Communication defined by the United Nations Commission on International Trade Law (Manzar & Chaturvedi, 2017). The act defines provisions regarding the protection of individual data. The sub-sections address definition of individual data, utilisation of individual data by site administrators and third parties, rights of users in case of data violation, and mechanism for dispute regarding privacy (Venkat, 2014).

The Act defines personal information as the "information about any existing person which may contain any specific code, sound, and/or image, which allows the possibility of an individual identification by name and official registration number including data which if not by itself permits for the possibility of detection when shared with other random information" (Abraham, 2009). As a governing measure, the commission on e-Privacy, run by the Ministry of Information and Technology (Government of India) offers code of conduct for web administrators (Acharya, 2014). The criteria for e-privacy commission to give legal structure to web based companies also examines whether companies meet the terms of the Information Protection Act, (Bélanger & Crossler, 2011). India also has various collateral agreements with other nations on technology development for online privacy (Al Hasib, 2009).

Website developers' responsibility: Self-regulation

Social media administrators must be responsive towards the public's concern over social media privacy and data protection. They must even respond with appropriate actions when required (Angulo, Hübne, Wästlund, & Pulls, 2012). In order to avoid legislative penalties, in 2003, all the major social networking administrators undertook to self-regulate their respective portals with the use of fair and transparent privacy practices for information sharing on their respective portals which includes: clearly posting their entire privacy rules on the respective sites, encoding user information, and taking part in accreditation programs from government regulatory agencies (Christofides, Muise, & Desmarais, 2009). However, the core of such responsibilities has been negligent. Reports claim that website developers' self-regulatory measures are on the decline and far away from government regulatory measures for user privacy protection rights (Cranor, 2003). These results led to the privacy regulatory body to review its previous proposals against legislative regulations and to give the verdict that due to ineffective efforts from website administrators, 'right to privacy' was added as a fundamental right for the citizens of India. The general public likewise wants government and judicial regulation to ensure users' online privacy protection (Mathias & Kazia, 2015).

Government's responsibility: Judicial regulation

In the case of Kharak Singh V. State of Uttar Pradesh (2015), the honourable Supreme Court of India specifically recommended that future judicial regulation should incorporate few basic standardised privacy principles for citizens of India. However, immediately after this case, the government took responsibility in 2015; a new committee was formulated to establish necessary online privacy legislation (Mahapatra & Choudhary, 2017). Fair Information Practice Principles (FIPP) laid the foundation steps for privacy standards in India. The government affirmed that it might be too early to endorse internet privacy as regulated and declare it as a fundamental right and the government perhaps should deliberate actions for more vigorous enforcement and legislation of present privacy bylaws (Kaushik & Tiwari, 2017). Supreme Court of India recommended that more analysis of privacy legislation should be considered and privacy protection laws should recommend that users' online privacy standards need not be different from offline privacy laws (Basu, 2017). Regardless of the government legislative actions, Supreme Court has also proposed various forms of regulations to uplift the privacy security in the country and in August 2017, a nine-judge panel gave a landmark judgment that "There is a need to maintain the core of an individual's privacy" and ruled that 'Right to Privacy' is intrinsic to life and liberty and intrinsically protected under the fundamental rights of the Indian Constitution (Duggal, 2017).

Literature review

Collecting and building user databases have become progressively frequent among web administrators. On the other hand, users are getting more personalized social platforms. However, users feel uncomfortable with the ease of changing the privacy settings (Awad & Krishnan, 2006). Past research studies have stated the elements that users consider significant with reference to social networking privacy; these include whether website administrators use individual data for commercial purposes and any mechanism provided to users to check how website administrators use their individual information (Berman & Bruening, 2001). There should be transparency about individual data collected, certifications of the websites, and users should have the facility to modify how individual data is viewed when required (Culnan & Armstrong, 1999). Previous studies concluded that participants were unconcerned about privacy on social networking sites; thus, their perspective towards online privacy was also lenient, but due to various high end online privacy scams, now users are very concerned about their privacy as well as read the available privacy statements on the respective social networking sites (Cho, Lee, & Chung, 2010). Despite users' huge concern about social networking privacy, surveys claim that users rarely read the privacy statements posted on websites and a large portion of users still do not know what individual information is stored and how it is used by website administrators (Gudura, Cranor, & Arjula, 2006). Since users rarely read statements associated with privacy and such statements perhaps do not precisely guarantee the implementation of privacy protection, the degree to which the site requests personal information from users at the registration process can be used for upgrading privacy protection standards (Korzaan, Brooks, & Greer, 2009).

The theory of social behaviour indicates that users reveal their personal data on websites in exchange for enlarging their social networks (Li, Wang, Li, & Che, 2016). Research studies specify that the ease which users feel with releasing data depends on the type of data asked from the users (Rotenberg & Scott, 2015). Users feel most awkward revealing information to website administrators about personal numbers, salary, medical history, residence information, demographic profile, and email address, in that specific order (Sheehan, 2002). However, to obtain commercial benefit, web portals may gather personal data from users (Smith, Milberg, & and Burke, 1996). Because of stringent protection laws, the Indian constitution forces limitations to how much data web portals can gather from users. The Information Technology Act 2000 proposes information minimisation (Cai & Gantz, 2000). This law expresses that asking of individual information must be limited to the least important elements. Even international laws indicate certain sorts of individual data, including medical records, political belief system, or religious convictions, as touchy individual data, and limit web portals from gathering such information (Han, Chang, & Kim, 2001). In any case, nations need stringent principles that oversee how much data and expansiveness (what volume of various points of data) of user data are being gathered by web portals '(Graber, DAllessandro, & Johnson, 2002).

The present study assesses whether web portals provide information while accessing data from users and whether users are provided with selection options for their respective privacy settings. For that, a few questions need to be addressed i.e., how users are notified about the data they provide to web portals (Vila, Greenstadt, & Molnar, 2003). As per a study on social media users in 2009, users are more inclined to peruse the privacy settings even if the web portals are not pushing for an effective privacy arrangement (Bellman, Johnson, Kobrin, & Lohse, 2004).

User data sought by web portals may vary as per the type of administration that web proprietors design. In this way, the accompanying exploratory questions are examined:

RQ1: Are the notified privacy policies by web proprietors sufficient to alleviate the concerns of the user?

RQ2: What are the implications of social web proprietors providing privacy selection options to users?

Legislation and privacy

Different nations adopt different strategies for data protection. Administrative methodologies with respect to data security assurance can be classified as: (1) legislative security and (2) industry self-control. Various nations, including Canada, Australia, European Union, and New Zealand implement the first approach. The European Union, which perhaps has the world's most stringent laws on data security, has laws that impact gathering, stockpiling, and utilisation of individual information (Papacharissi & Fernback, 2005). The laws require authorisation for web portals and governments to gather, exchange, offer and utilise individual information (DeMarco, 2006). In the meantime, a few nations have developed industry self-control mechanism without larger participation by laws directing data security. Self-control measures by industries provide guidance for gathering and utilisation of individual data to site proprietors (Cassidy & Chae, 2006). Authorities for internet businesses in a few nations are worried that government mediation and endeavour to secure users could discourage the interests of the users. To drive development of internet businesses, nations like America have endeavoured to limit government mediation via employing self-control method (LaRose & Rifon, 2007). The effectiveness of self-control depends on the awareness of users, as they would deliberately maintain a strategic approach for social media sites and criticise security arrangements that encroach on their protection ' (OConnor, 2007). Users will move to social networking sites that present more grounded protection insurance. If a specific website does not secure data protection, users with strong self-privacy concerns would move away from such sites. Social media users contend that effective privacy settings are required as users don't want commercialization of their personal data which may be used to manipulate their decisions (Turow, Hennessy, & Bleakley, 2008).

Information and Technology Act 2000 deals with privacy policies in India, This act provides rules for individual data protection. The rules are based on standards prescribed by the United Nations. They address rules for individual data usage as well as storage of individual data, and the utilisation of individual data interactions in their respective groups (Angwin, 2011). The Act alludes to individual data as the data of a registered user which may include the code, name and additionally picture that helps a person to be distinguished from others (Hansen & Jespersen, 2013). The policy adopts the self-direction strategy regarding consumer security on the web. Under the self-control method to deal with data protection, India had never approved any act before 2017 which governs data security practices of online businesses. However, online businesses in India are urged and informally required to take after the data security rules of the International Trade Commission (Hagman, Andersson, Vastfjall, & Tinghog, 2015). The commission gives reasonable standards for data practices as models to regulate privacy of the user with the scope for marketers to get benefits from the user data. The models give standards with respect to assent, access, and security of purchasers' information that is gathered (Wu, 2014). Lately, major online organisations, for example, Facebook and Google were alleged to have abused user information or gathered information in unethical ways (Dinev & Hart, 2006). In particular, numerous applications on Facebook have transmitted individual data of users to third parties. Google's Street View autos gathered individual data from decoded Wi-Fi systems, and Google Buzz likewise uncovered clients' individual data to different people for commercial purposes. These cases created the perception that web portals don't monitor their actions viably as per the self-direction method (Fogel & Nehmad, 2009). Thus, various international administrations are enforcing new laws that direct web portals regarding accumulation of individual data (Solove, 2001). As for online frauds in India, the India Ministry of Information and Technology is working on the Internet Protection bill. In 2015, Government of India representatives proposed an enactment to make a bill named the Bill of Privacy Rights Act (Tan, Qin, Kim, & Hsu, 2012). While the previous privacy laws cover the protection of only certain kinds of confidential individual data, for example, demographic and money related data, this proposition would deliver the country's first more secure protection laws (Gauzente, 2004).

The bill provides users better access over the utilisation of their own information and the capacity to control how the data is utilised or disseminated. Likewise, the bill expects internet based organisations to get authorisation from users before gathering and sharing confidential demographic, health, and monetary information with third parties (Hiller, Smith, & Bélanger, 2002). Considering the need to re-structure the existing privacy policies, Indian national associations have started to think about the acts by which courts can execute better privacy frameworks while protecting data on social networking sites. The ineffectiveness of legal structures, bounding the capacity of judiciary to detain and question web portals on ineffective strategies for data management, authors urge that there is a need for better policy with regards to privacy on social media. Akar & Topcu (2011) claim that legislative ability to enforce law on the web portals would enhance security for users; legislative aptitude incorporates policymakers' capacity to recognise administrative challenges, create approachable platforms, form

laws and execute them to give capable privacy settings. In any case, building a worldwide privacy control technique requires a dynamic approach providing users to make modifications whenever required. This study inspects the adequacy of the Indian government's present ways of dealing with data security and the current security offered to users of Indian websites (Nissenbaum, 2004). To do so, this study utilises the rules of the Indian Directive for Data Protection as it is more generalized, considering each of the five data security aspects: notify, selective, security, modified, and legitimacy.

The level of privacy concern may be different from user to user. Along these lines, this research study assesses the contrasts regarding the different users for privacy concerns. It likewise analyses the connection between web portals' security approaches to privacy concerns of clients(Karyda, Gritzalis, Park, & Kokolaki, 2009).

RQ3: Do the privacy setting modification options have any impact on the individual user's account on the website?
RQ4: The impact of the security structure on the website on the individual's concerns regarding security.
RQ5: The impact of the legislation structure provided by the government and judiciary on the user's concerns about privacy.

Research Methodology

Sample and procedures

The average age of respondents was 22.4 years (Standard Deviation = 2.45, range = 20–32, Median = 21.0). Out of the total number of respondents N= 352, Female respondents (n = 216, 66.46%), outnumbered male respondents (n = 136, 33.53%, 1 missing value). Considered participants were active social networking users, with 75.2% (n = 264) having one or more social networking profile and 89.4% (n = 315) accessing their preferred social networking site at least once in a day. To explore the research objectives, an in-depth analysis of web portals in India was carried out. To investigate how leading web portals execute privacy settings, the current research chose the 20 most visited web portals from India. The selection was based on the rankings (number of users) of websites (Diephay, 2016). The rankings were surveyed by the quantity of users amid the given timeframe. Out of the main 20 social networking sites, a portion of the websites was rejected from the selected web destinations. The justifications for rejection were: (1) Web destinations without an enlisted privacy strategy, (2) online enrolment that pre-requires an offline enrolment (i.e. mobile registration), (3) web portals under development, and (4) web portals that involve monetary instalment for enrolment. Web portals with such criteria were removed from the research framework. The investigation utilized an aggregate of 8 web portals for this research examination i.e. Facebook, Instagram, LinkedIn, Google+, Twitter, YouTube, Pinterest and Tumbler. For all the chosen web portals, content was examined and the author analysed the operational privacy mechanism of each web portal to understand the privacy definitions of each web portal. After this step, a pre-test was conducted on a few (N=50) social networking users to validate the chosen variables. For the pre-test, 25% of web portals incorporated into the example were arbitrarily chosen utilising a random selection strategy. In view of the reliability and validity check, Cronbach's alpha test was executed for the dependability trial of the scale, and it was ascertained that Cronbach's alpha = 0.682. This figure demonstrates that the scale is profoundly solid for examination.

Hypotheses and Proposed model

The intent of this study was to explore the impact of various identified factors on users' privacy concerns on social networking sites. The determinants of users' privacy policy have been arranged into 5 fundamental measurements:

H1 : Notification of privacy settings on a web portal by the web administrator affects privacy concerns of the user.
H2 : Selection of privacy related settings on a web portal by the web user affects privacy concerns of the user.
H3 : Availability of modifications of privacy related settings on a web portal affects the privacy concerns of the user.
H4 : Internal securitization of privacy related settings on a web portal affects the privacy concerns of the user.
H5 : Legislative structure for privacy related settings on a web portal affects the privacy concerns of the user.

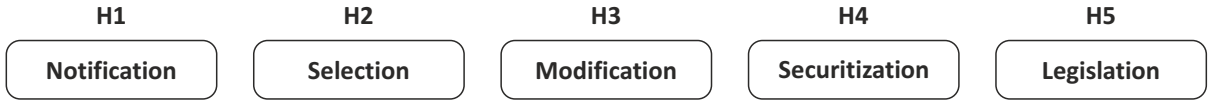

Figure 1 Conceptual framework for the study

Source: Author's Compilation

Findings

RQ1: Notification of privacy settings on a web portal by the web administrator affects privacy concerns of the user: With respect to notification of privacy settings, over 90% of the Indian web portals provide notification about the privacy structure of the web portal for registration. In comparison to rest of the world, around 95% of the web portals provide notification about privacy settings. Most of the Indian web portals also require gender (89.0%) and date of birth (82.0%) along with month of birth (81.3%), year of birth (88.9%), and email address (84.6%). Surprisingly, 79.21% of Indian web portals request a code-based registration number which is sent via email or mobile as a requirement for registration. With respect to social networking sites, pop up privacy notification (92.7%) was the most frequently used notification method for enrolment followed by email (57%). One-way ANOVA was performed to understand the impact of notifications for privacy in the selected social media profile. The ANOVA result showed that Facebook (Mean=3.53, SD=1.17) on the scale of 1 to 5 (where 1 means least bothered and 5 means highly bothered) provided a significantly higher concern for privacy than LinkedIn (Mean= 2.89, SD=1.76). With respect to overall results, web portals providing notifications for the privacy of the user account on the specific account significantly affected privacy concerns of the user (F value=26.80, DF=351, p value <0.001).

RQ2: Selection of privacy related settings on a web portal by the web user affects privacy concerns of the user: The second research question asked was whether availability of selection of privacy settings by the website administrator affects the privacy concerns of users. There are differences between various selected web portals in terms of amount of selection options provided to users. One-way ANOVA was performed to compare the selection options of the web portals based on the selected social media profile. The ANOVA result showed that LinkedIn (Mean=3.46, SD=1.38) on the scale of 1 to 5 (where 1 means least bothered and 5 means highly bothered) provided significantly more methods of privacy selection options than Facebook (Mean= 3.12, SD=1.4). With respect to overall results, social networking sites providing selection options for the privacy of the user significantly affects the privacy concerns of the user (F value=30.94, DF=351, p value <0.001).

RQ3: Availability of modifications of privacy related settings on a web portal affects the privacy concerns of the user: The third research question addressed whether web portal privacy settings modification triggered a difference in the extent of privacy concerns. The study employed ANOVA to answer the question. The results from ANOVA discovered that there is statistically a significant difference if options of modification of the privacy structure of the web portal are made available to users. In other words, social networking sites of all examined genres were requested to have a flexible structure for privacy options of the user. In the analysis of the major web portals i.e. Twitter, Facebook, etc. showed that there are statistically significant differences among web portals' privacy settings modification with respect to privacy concerns (F value=5.76, DF=6.87, p value>0.001). To investigate the differences among web portals genres individually, Bonferroni post-hoc analysis was executed. The results show that modifications on privacy settings (Mean=8.42, SD=5.56) requested more freedom to the user which resulted in positive outcomes on their privacy concerns.

RQ4: Internal securitization of privacy related settings on a web portal affects the privacy concerns of the user: Research question four asked whether the securitization structure available on the site had various levels of privacy protection. One-way ANOVA was conducted to test the difference between the securitization and non-securitization of web portals on the privacy concerns of the user. In general, web portals without security structure (Mean value=1.11, SD=2.99) presented negative results. The results show strong security components of privacy protection policies significantly impact the privacy concerns of individuals. When evaluating the answerability dimension, Instagram was less probable than Facebook to specify user information and independent resources for probable privacy problems. LinkedIn users (61.8%) were more likely than Facebook users (21.8%) to offer data regarding their education, occupation and income level. On the other hand, Twitter (54.0%) users were less probable than Facebook (86.1%) users to share their information with third parties (R^2=40.54, DF=10, p value <0.001).

RQ5: Legislative structure for privacy related settings on a web portal affects the privacy concerns of the user. Research question five is concerned with the legislative structure for privacy protection policies among websites. Two separate ANOVA tests were conducted for each website. Survey of Facebook and Instagram signified that there is no major difference among various social networking sites with respect to the overall level of privacy legislative structure. When considering each component of privacy legalization policies, the Chi-square test results indicated that there were statistically significant differences among websites genres with respect to the notification regarding the type of information collected (R^2=13.30, DF=10, p value >0.05), the purpose of the information use (R^2=12.80, DF=10, p value>.05), third-party disclosure (R^2=27.66, DF=10, p value>0.001), and use of cookies (R^2=13.99, DF=1, p value>0.05). In contrast, the review of legislative aspect on websites did not expose any significant difference in the level of individual dimension of privacy concern.

Generalizability and Applicability

The findings and implications from this research study are quite expansive. Though this study has been conducted in India, we can generalize the findings in other emerging economies. This is because all the respondents chosen have similar behavioural patterns with all other countries. There are no/very negligible differences in the privacy policies, practises, and guidelines between countries across the world. Any individual respondent will demonstrate considerable homogeneity of privacy policy, guidelines, and practices across all social media platforms throughout the world (Srivastva & Sharma, 2020). The findings from the analysis of processes, policies and practises of one country can be generalized for other countries. A large chunk of the sample, that is, social media users for most social media sites are frequently subjected to privacy concerns. This is to say that the respondents in the sample have varied privacy breach experiences in various social media handles as well as in various geographical locations across India. Hence, we can conclude that the findings can be quite conveniently applied to other parts of the world. The digital world today has become one global village. As such, the broad digital objectives of improved security and enhanced quality of service in order to achieve transparent competitive advantage remain the universal and core target of all social media sites irrespective of their genre. The study has emphasized on social media sites enhancing empowerment of users which is a prerequisite for enhanced transparency for both formal and informal users (Sharma & Kurein, 2018). Privacy concerns have become a vital antecedent for users to register and use a social media site not only in India but also in other emerging and developed economies. Again, the research study has demonstrated that site policies, nature of user, judicial environment and modification options favourably impact attainment of privacy. Privacy concerns are universal across all users and need to be addressed to ensure satisfaction of users. Most social media sites have strict privacy settings. Most users even utilize these settings in order to protect their individual data. Thus, the findings can hold true and applicable for social media sites functioning in all types of economies – developed, evolving or evolved. The relationship established in this study is based on various practises and processes prevalent on social media sites and not on any behavioural outcomes of the users concerned. Social media administrators can conveniently replicate the policies and processes mentioned in the study in other countries.

Conclusions and Suggestions

The current research highlights literature on users' data privacy in India. In India, internet-based organizations demand more diverse types of information than in other countries. The differences in the volume and extent of user data requested were also deceptive on selected web portals. The eight considered social networking sites requested for extensive information. The investigation reveals insights on the connection between privacy concerns of users and user data sought by web portals. Social networking site Facebook has structured data privacy settings compared to other websites. A comparison with seven other social networking sites reveals that Facebook seeks more personal data from users. With respect to privacy protection strategies, in India, social networking sites exhibited lower protection assurance compared to the rest of the world. Users on social networking sites appreciate the notification of privacy settings. Different social networking sites had different levels of notification display; however, those with higher display of notifications and security generated higher user comfort and security. Websites that permit users to opt in and modify privacy settings have more satisfied users in terms of privacy. Web portals must notify with explanations their decision to give third parties access to data, data transfer, data mining, and commercial usage. In-depth analysis of websites uncovered no major difference in privacy policies as per website statements, but there is a conceivable difference amongst the various sites in terms of how web portals notify particular privacy settings. However, it is suggested that India should improve privacy approaches for data usage as per the standards and rules of the international lobby. This investigation likewise suggests restructuring of the legislative approach towards data protection in India. India's laws relating to data privacy on social networking sites are lax. While this gives users more opportunities, it permits website administrators to be careless about user data. A fully explained and modifiable introduction of privacy settings on web portals ought to be a fundamental for positive privacy concerns of the users. Notification of privacy settings on Indian web portals was poor compared to those on international sites. Since this study covers a limited number of social networking sites, generalizability of its findings is limited. However, it is conceivable that the selected web portals for this examination don't follow effective data protection strategies. In view of the findings of the present investigation and previously mentioned literature for online privacy, administrators of web portals should enhance the privacy standards as per the global standards. Future studies can additionally investigate various other aspects of social media users with reference to privacy concerns.

References

- Abraham, S. (2009). *Section 66A of the Information Technology Act.* Bengaluru: Kusuma Trust.
- Acharya, B. (2014). *Open Call for Comments: The Privacy Protection Bill 2013 drafted by the Centre for Internet and Society.* New Delhi: The Centre for Internet and Society.
- Al Hasib, A. (2009). Threats of online social networks. *International Journal of Computer Science and Network Security, 9* (11), 288-293.
- Angulo, J., Hübne, S. F., Wästlund, E., & Pulls, T. (2012). Towards usable privacy policy display and management. *Information Management & Computer Security, 20* (1), 4-17.
- Angwin, J. (2011). Senators offer privacy bill to protect personal data. *Wall Street Journal, 3* (1), 23-30.
- Awad, N., & Krishnan, M. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *Management Information Systems Quarterly, 30* (1), 13-28.
- Basu, I. (2017). *Right To Privacy Is A Fundamental Right Under The Indian Constitution.* New Delhi: HuffPostIndia.
- Bélanger, F., & Crossler, R. (2011). "Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly, 35* (4), 1017-1042.
- Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20* (5), 313–324.
- Berman, J., & Bruening, P. (2001). Is privacy still possible in the twenty-first century? *Social Research, 68* (1), 306-318.
- Bryce, J., & Klang, M. (2009). Young people, disclosure of personal information and online privacy: control, choice and consequences. *Information Security Technical Report, 14* (3), 160-166.
- Cai, X., & Gantz, W. (2000). Online privacy issues associated with Web sites for children. *Journal of Broadcasting & Electronic Media, 44* (2), 197-214.
- Cassidy, C., & Chae, B. (2006). Consumer information use and misuse in electronic business: An alternative to privacy regulation. *Information Systems Management, 23* (3), 75-87.
- Charters, D. (2002). Electronic monitoring and privacy issues in business marketing: the ethics of the doubleclick experience. *Journal of Business Ethics, 35* (4), 243-254.
- Cho, H., Lee, J., & Chung, S. (2010). Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26* (5), 987-995.
- Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *Cyber Psychology & Behavior, 12* (3), 341-345.
- Cranor, L., (2003). P3P: making privacy policies more useful. *IEEE Security & Privacy, 1* (6), 50-55.
- Culnan, M., & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. *Organization Science, 10* (1), 104-115.
- Dasgupta, S. (2018). *How the likes of Cambridge Analytica can change politics.* New Delhi: The Economic Times.
- DeMarco, D. (2006). Understanding consumer information privacy in the realm of Internet commerce: Personhood and pragmatism, pop-tarts, and six-packs. *Texas Law Review, 84* (1).
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17* (1), 61-80.
- Duggal, P. (2017). *Right to Privacy Judgment: The Long and Short of It in 21 Points.* New Delhi: The Quint.
- Fogel, J., & Nehmad, E. (2009). Internet social network communities: risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25* (1), 153-160.
- Gauzente, C. (2004). Web merchants' privacy and security statements: how reassuring are they for consumers? A two-sided approach. *Journal of Electronic Commerce Research, 5* (3), 181-198.

- Graber, M., D'Allessandro, D., & Johnson, W. J. (2002). Reading level of privacy policies on Internet health Web sites. *Journal of Family Practice, 51* (7).
- Gudura, P., Cranor, L., & Arjula, M. (2006). User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction, 13* (2), 135-178.
- Hagman, W., Andersson, D., Vastfjall, D., & Tinghog, G. (2015). Public views on policies involving nudges. *Review of Philosophy and Psychology, 6* (1), 439–453.
- Han, J., Chang, H., & Kim, J. (2001). The status of personal information protection policies on e-commerce websites. *Journal of Information Protection, 11* (4).
- Hansen, P. G., & Jespersen, A. M. (2013). Nudge and the manipulation of choice: A framework for the responsible use of the nudge approach to behaviour change in public policy. *European Journal of Risk Regulation, 4* (1), 3–28.
- Hiller, J., Smith, W., & Bélanger, F. (2002). Trust worthiness in electronic commerce: the role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11* (3), 245-270.
- Hong, W., & Thong, J. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. *Management Information Systems Quarterly, 37* (1), 275-298.
- Karyda, M., Gritzalis, S., Park, J., & Kokolaki, S. (2009). Privacy and fair information practices in ubiquitous environments: research challenges and future directions. *Internet Research, 19* (2), 194-208.
- Kaushik, K., & Tiwari, R. (2017). *A to Z of Privacy.* New Delhi: The Indian Express.
- Korzaan, M., Brooks, N., & Greer, T. (2009). Demystifying Personality and Privacy: An Empirical Investigation into Antecedents of Concerns for Information Privacy. *Journal of Behavioral Studies in Business, 1*, 1-17.
- Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks:why we disclose. *Journal of Information Technology, 25* (6), 109-125.
- LaRose, R., & Rifon, N. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs, 41* (1), 127-149.
- Li, K., Wang, X., Li, K., & Che, J. (2016). Information privacy disclosure on social network sites. *Nankai Business Review International, 7* (3), 282-300.
- Lowry, P., Cao, J., & Everard, A. (2011). "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, 163-200.
- Mahapatra, D., & Choudhary, A. A. (2017). *Right to Privacy is a fundamental right, it is intrinsic to right to life.* New Delhi: Times of India.
- Manzar, O., & Chaturvedi, U. (2017). *It's Hard to Understand Privacy in India.* New Delhi: https://thewire.in/.
- Mathias, S., & Kazia, A. N. (2015). *Data protection in India: overview.* New Delhi: Department of Electronics and Information Technology.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79* (1), 101-139.
- O'Connor, P. (2007). Online consumer privacy: An analysis of hotel company behavior. *Cornell Hotel and Restaurant Administration Quarterly, 48* (2), 183-200.
- Papacharissi, Z., & Fernback, J. (2005). Online privacy and consumer protection: An analysis of portal privacy statements. *Journal of Broadcasting & Electronic Media, 49* (3), 259-281.
- Rosen, J. (2001). Out of context: the purposes of privacy. *Social Research, 68* (1), 209-220.
- Rotenberg, M., & Scott, J. (2015). *Privacy in the Modern Age: The Search for Solutions.* New York: The New Press.
- Sheehan, K. (2002). Toward a typology or internet users and online privacy concerns. *Information Society, 18* (1), 21-32.
- Smith, H., Milberg, S., & Burke, S. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167-196.
- Solove, D. (2001). Privacy and power: computer databases and metaphors for information privacy. *Stanford Law Review, 53* (6), 1393-1462.

- Stewart, K., & Segars, A. (2002). An empirical examination of the concern for information privacy instrument, *Information Systems Research, 13* (1), 36-49.
- Sumanjeet. (2002). Cyber laws in need of upgrade. *Indian Business Law Journal, 1* (2), 27-29.
- Tan, X., Qin, L., Kim, Y., & Hsu, J. (2012). Impact of privacy concern in social networking web sites. *Journal of Internet Research, 22* (1), 211-233.
- Turow, J., Hennessy, M., & Bleakley, A. (2008). Consumers' understanding of privacy rules in the marketplace. *Journal of Consumer Affairs, 42* (3).
- Venkat, V. (2014). *India violating privacy of Internet users.* CHENNAI: http://www.thehindu.com/.
- Vila, T., Greenstadt, R., & Molnar, D. (2003). Why we can't be bothered to read privacy policies: Models of privacy economics as a lemons market. *50.* New York: ACM Press.
- Wu, X. (2014). Data Mining with big Data. *IEEE Transactions on Knowledge and Data Engineering, 26* (1), 27–29.

Ravneet Singh Bhandari *is pursuing his Ph.D. in Management from Amity University. He has an MBA from Symbiosis University and PGDBM from IGNOU and BBA from GGSIP University. Ravneet is Professor of Marketing and International Business at Amity University. He teaches Management at both the graduate and undergraduate levels. His areas of expertise include digital marketing, social media marketing and SEO. In addition to his academic duties, Ravneet works as a freelance marketing expert for various clients. Ravneet serves on the reviewer board of various Scopus indexed and ABDC listed journals and has published over 25 articles in Scopus indexed, ABDC listed and Web of Science indexed academic journals and authored a book on PPC strategies by Lambert Publications. He regularly conducts research paper reviews for various publishers. His current research activities are varied and include work on the determinants of digital marketing. He can be reached at rbhandari.vf@amity.edu, ravneetsinghbhandari@gmail.com.*

Sanjeev Bansal *is Dean of faculty of Management Studies, Director of Amity Business School in Amity University, Uttar Pradesh. He has a Ph.D. and D.Litt. His doctoral research was an exemplary work in this field. He is in the field of academics for more than 3 decades. He is associated with Amity University for more than 14 years after serving in the University of Delhi. He has established and looked after the Doctoral programme of ABS since its inception. He has guided more than 300 dissertations and projects. He has 32 books and more than 170 research papers to his credit. 24 students have completed their M. Phil / Ph.D. under his guidance and 8 students are presently pursuing their doctoral work under his supervision. He is on academic / advisory bodies of many institutions and universities. In his pursuit of excellence, he has explored many B. Schools of India and travelled to well-known Business schools abroad such as Wharton, New York University, Wagner, and Harvard. During his distinguished career of over 30 years, he has many distinctions in the field of academics and is well known as an institution builder, an acclaimed teacher and an avid researcher. He can be reached at sbansal1@amity.edu.*