Information privacy concern at individual, group, organization and societal level - a literature review

Dillip Kumar Rath and Ajit Kumar
Department of Information Systems, Xavier Institute of Management, Bhubaneswar, India

Received 24 August 2020
Revised 19 October 2020
Accepted 11 December 2020

Abstract

Purpose – In today's digitized environment, information privacy has become a prime concern for everybody. The purpose of this paper is to provide an understanding of information privacy concern arising because of the application of computer-based information system in the various domains (E-Governance, E-Commerce, E-Health, E-Banking and E-Finance), and at different levels, i.e. individual, group, organizational and societal.

Design/methodology/approach – The authors performed an in-depth analysis of different research articles related to information privacy concerns and elements affecting those at certain level of applications. The primary sources of literature were articles retrieved from online databases. Various online journal and scholarly articles were searched in detail to locate information privacy-related articles.

Findings – The authors have carried out a detailed literature review to identify the different levels where the privacy is a big challenging task. This paper provides insights whether information privacy concern may obstruct in the successful dispersal and adoption of different applications in various application domains. Consumers' attitude towards information privacy concerns have enlightened and addressed at individual levels in numerous domains. Privacy concerns at the individual level, as suggested by our analysis, seem to have been sufficiently addressed or addressed. However, information privacy concerns at other levels – group, organizational and societal levels – need the attention of researchers.

Originality/value – In this paper, the authors have posited that it will help the researchers to more focus at group level privacy perspective in the information privacy era.

Keywords Information privacy, Information security, Information privacy concern, Privacy levels

Paper type Literature review

Introduction

The deployment of computer-based information system (CBIS) is continuously increasing in various spheres of human life, such as education, health care, commerce, transportation, governance, the social network and various other areas. The purpose of CBIS deployment is to make information processing, storage and sharing with effective and efficient (Yadav, 2006). Undoubtedly, the CBIS applications have brought convenience and efficiency to daily human life by collecting, processing and communicating users' information. There are two major

concerns of individuals came in to picture, i.e. privacy and security, when their information stored and processed in the CBIS.

Privacy and security concern

In the CBIS, the service provider collects information about individuals and uses it for analytics (Straub and Collins, 1990). They use those resources to design and develop new products. The design of modern CBISs allows the system to pry on all the activities of an individual continuously. With communicated technologies, data can be collected, stored and reused to a significant volume (Malhotra *et al.*, 2004). As computers, networks, mobile devices are increasing the use of communication, business process automation and other facets of life; privacy is becoming a concern of high importance. While the applications bring convenience to daily life, different agencies also collect information regarding the users, which is necessary to tailor the information to bring convenience. The data gathered about individuals might be used even without the consent of an individual. This information gathering and storage has raised two main information concerns:

(1) Security concern

(2) Privacy concern

Security concern. Security is a fundamental component in any transaction data processing system. Security is a robust requirement in all computing systems (Gonzalez *et al.*, 2012), and this is a significant concern in today's current progressive environment. We considered that security is a concern where all information is stored and used for analytics purpose. Nowadays, security is a significant challenge in protecting individual information (Straub and Collins, 1990). The security concern has direct implication towards resource sharing. Moreover, at this point security concern deals with sources of information to be kept and used by the right person, right time, right value and right location (Burton *et al.*, 2012) with efficiently and effectively. Any security breaches will lead to the mishaps in the whole system.

Privacy concern. Privacy is an intangible apprehension of an individual property. Privacy is someone or something, which is not observed or disturbed by others – "an individual right to keep the personal information and matters secret and control over the information". Privacy may also is a state free from unwanted intrusions and disturbances; the ability of an individual to certain ways publicized in a specific way (Fried, 1968). Private to individual means something is unique and sensitive to them. Vocabulary such as private, isolation, quietness, interruption, intrusion and lack of disturbances, characterizes individual privacy. It may be connected directly or indirectly with a person's ownership of information and control over sharing mechanism. In general, individuals are more concern towards information privacy concern due to their engagement and the growing habitat nature towards adopting the new technologies. The privacy of resources which have a value needs to be protected. So, privacy concern raised by individuals is a significant issue in the context of the information storing, analysing, sharing and maintaining in CBIS. Figure 1 highlights the overview of information privacy at different stakeholders.

Literature review

We performed an in-depth analysis of information privacy concerns (IPC) by searching for various research articles from online peer-reviewed journals. We reviewed the literature to

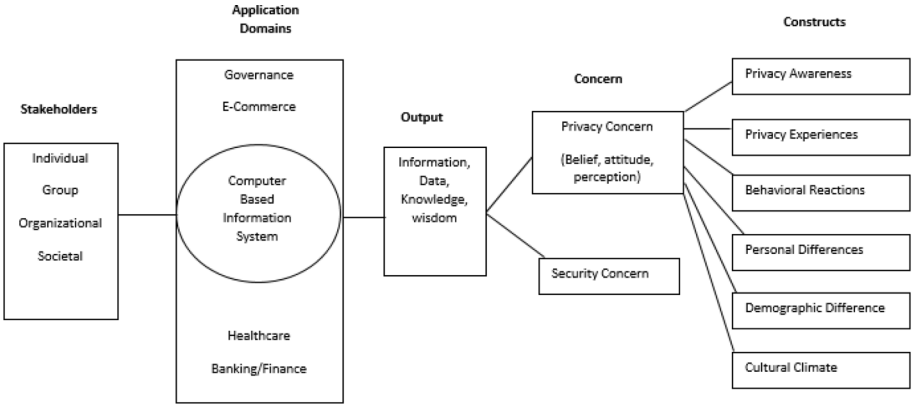

Figure 1. Overview of information privacy at different stakeholder's levels

understand the status quo of this issue around the world. Keywords combinations, such as "privacy concern," "privacy concern of information system", "data privacy and electronic system", were used to find relevant literature. A total of 124 literature related to information privacy concern have been reviewed, and 84 scholarly articles were found to be fit for our review and analysis, and hence, taken into consideration.

The objective of this review is to provide a concise but clear picture of information privacy concern (IPC) in an information system environment at different levels and different domain applications around the world. Some research papers focus on concern for internet privacy, digital privacy, the multilevel effect of information privacy and internet purchasing behaviour related to privacy concerns. Privacy-related research has a cultural dimension, and most research has focused on the western context. Through this cross-sectional view of information privacy concern (IPC); this paper aims to provide a better picture of information privacy concern at different levels. Table 1 profiles the definitions of information privacy concern.

Privacy concern in various domains

In this study, we have tried to analyse the interrelationship and the influencing factors affecting the privacy concern and how different applications are associated with privacy concerns. Privacy concern is of the utmost importance for applications like health-care domain, banking, governance, e-commerce, financial institutions, the internet, cloud computing, social networking and education. Privacy concern on different domain applications are as follows:

E-business

Electronic business (E-business) refers to transforming business transactions through the internet. These business transactions include a process in buying and selling, customer service, managing process on production, payment processing, collaboration with trading partners (Swani and Brown, 2011). The financial privacy (Jentzsch, 2001) is related to an individual's financial transactions are recorded with the proper process, and it ensures that all information to be covered by avoiding fraud. However, the actual required personal identifying information is collected using a certain mining software (Li and Sarkar, 2006). In social contract theory, (Donaldson and Dunfee, 1994) researcher explained the privacy concern by which the fair means of a collection of personal information on the web through

S.N.	Source/Author	Definition
1	Warren and Brandeis (1890)	Right to be alone in the right to privacy described as the right of a person to be alone by isolation from the attention of others
2	Fried (1968)	An individual right to keep the personal information and matters secret and control over the information and also privacy may be explored as a state free from unwanted intrusions and disturbances; the ability of an individual to select to be publicized in a certain way
3	Westin and Louis (1970)	Information privacy is the ability of a person who has control over the data and to what extent the data would communicate to others
4	Posner (1983)	Information privacy as an option to secrecy by that everyone has the right to restrict the information about themselves in public and where outsiders should not be encouraged to take advantage of it
5	Kufer (1987)	Privacy can be observed with autonomy, a segment closely associated with personhood
6	Smith *et al.* (1996)	Information privacy is the relationship between technology and the individual's ownership of collection and sharing of data
7	Jentzsch (2001)	Financial privacy is related to a person's financial transactions are recorded with proper process, and it ensures that all information to be covered by avoiding fraud
8	Dinev and Hart (2004)	In internet privacy, the information of each concern would be kept preserved with more security by the utilization of new technology
9	Skinner *et al.* (2006)	Information privacy contexts examine the four dimensions of privacy: Personal behavior privacy, personal privacy, communication privacy and data privacy
10	Dinev and Hart (2006)	Information privacy concern explains the level of privacy with various dependent variables such as eagerness, willingness to provide the personal information over the internet. In general, individual perception of users, who are using the internet, be afraid in mind that what happens with the data they provided over the internet
11	Smith *et al.* (2011)	Information privacy is the relationship between technology and the individual's ownership of collection and sharing of data

Table 1.
Profiles the definitions of information privacy concern

online are only justified if the consumer given the preferences of control and the way of using that information. In a certain way, consumers are vulnerable towards the utility of their personal information (Culnan and Williams, 2009) and the inability to control over the information utilization.

Moreover, unknown to individual data can be collected, additional data without the individual being aware (Belanger and Hiller, 2006). Often data is shared for a particular purpose but ends up being used for an entirely different purpose. There is privacy paradox, where individual privacy information does not match actual behaviour when they are

sharing information (Norberg and Horne, 2007). In some cases, individuals prefer to state their actual information through online purchase (Brown and Muchira, 2004) when they find it convenient.

Health-care domain

The health-care system is the management of the organization, consisting of resources, policies, people and services, which dealt with to deliver health-related information to the people concern. Modern health-care system activities use information technology as a baseline to deliver better and effective service to citizens (Ovengalt *et al.*, 2017). Health-care practices cover with disease diagnosis, hospital activities and human health checkup. By the utilization of technology, it becomes easy to serve medical treatment with quality service by adopting new, developed infrastructural equipment (Raval and Jangale, 2016). The patient is in a state to provide all the necessary information to the concerned authority at the time of disease diagnosis (Tham *et al.*, 2014). However, fear factors arise in the mind of a patient, whether private information is kept confidential. This observation creates fear and reduces trust in the hospital practitioner. Here, trust plays a major role and form a different association between patient and practitioner.

Banking and finance domain

Privacy and security concerns in banking industries tend to be a significant concern at the individual level as well as organizational level. Individuals have good faith and trust in bankers (Omariba *et al.*, 2012) that their private data would never be made public. The banking system follows some standards which are a crucial concept to be maintained by every banker. In some cases, bankers themselves have breached the system and information has been leaked (Amor, 2002). To protect the privacy information of the customers, banks have taken major steps by formulating protection policy to accumulate the confidence of the customers (Normalini and Ramayah, 2017). Moreover, the bank also assured that, at any cost, the transaction record would not have transmitted to the public domain. Banks have committed to their privacy policies, not to disclose private and confidential information (Sohail and Al-Jabri, 2014).

Social networking

The current scenario shows that social networking has changed the way people communicate and their lifestyle. People interact with their friends, relatives and family members on a single platform, and this possibly poses a privacy risk (Alashoor *et al.*, 2017). The hackers access detailed private information from those social network sites (Kyei-BlanksonIyer and Subramanian, 2016) by sending the adware or malicious links, and they use it to transfer all that private information. So, it becomes a significant challenge to tackle in current scenario because social media and social networking sites are heavily accessible by the youth of many nations (Spottswood and Hancock, 2017). Maintaining privacy through the social networking site is the right of the individual to show the personal information, storing the personal information, access to third parties and displaying the information via the web (Black *et al.*, 2015).

Governance

In the recent trend of digital transformation over the internet, there are multiple opportunities available doing business and deliver excellent quality services. Nevertheless, as the information collected, processed, stored and analysed by the organizations

(Singh and Chauhan, 2012), it becomes an increasing challenge towards data security, information privacy and related state of compliance. A sound governance system is one where people are working together by using three resources together – human resource, information process and technology applications. In this connection, the privacy concern of everyone to be maintained by collecting and processing the personally identifiable information (Kharade, 2016) together by keeping the trade secret with confidential information. In general, technology is an integral part of information security, threat alert and risk management (Saha *et al.*, 2010). Employees concerned should have clearly defined roles and responsibilities, essential resources and clear guidance to handle the objectives of the organization (Martin, 2016).

Methodology

To present a concise and refined perspective, this paper considers not only scholarly articles on information privacy but also specific online resources which deal with privacy and security concerns. Useful articles from electronic databases like EBSCO, JSTOR, Taylor and Francis, SAGE, ProQuest, Elsevier (Science Direct), Google.com, Emerald and Google Scholar were accessed. Specific keywords like'Information Privacy','Information Privacy Concern','Levels of Privacy','Individual and Group Privacy', 'Dimensions of Privacy', 'Privacy and Security', 'Measure the Privacy Concern', 'Tools and Techniques for Privacy Concern', 'Indicators of privacy and measurement', 'Privacy Issues', 'Factors in Privacy Concern', 'Privacy Act', 'Multidimensional effect on Privacy' and other relevant words were used in different combinations to be as accurate as possible in getting the results. The preliminary search of results had thrown up many cases, of false results, so the search had to be refined. For example, specific search results dealt with other dimensions of privacy like culture, act and policy rather than with information privacy concern. Most of these false articles could be eliminated based on a brief reading of the title. We decided on the relevance of the other articles after a reading of the abstracts. Hence, in this paper, the literatures on information privacy concern are reviewed through four perspectives. First, there is a chronological study of literature, where the paper looks at how research on information privacy concern has developed and how different papers described the IPC. Second, this paper looks at how different application/area concern towards IPC and elaborate factors which influence IPC. Third, this paper looks at the various levels that have emerged in the field of information privacy concern, thus highlighting the different issues that people face in privacy concern at individual, group, organizational and societal levels. Finally, the paper looks at how the multilevel effect of analysis has progressed across different geographical nations and cultures. Several research articles describe and reflect on information privacy; that is, how various factors influence privacy concerns and what is the built-in relationship existed between them and how hierarchical multilevel effects influence others.

Result and discussion

Information is defined as a structured way of representation of the raw data after processing, summarizing and transforming. Data is processed, stored and shared in a certain way, and an arrangement meaningfully represents it. By the utilization of computer-based information system (CBIS), data is collected, processed, stored, analysed and transformed into a meaningful way. Information privacy is defined as the right of an individual over the personal data, who can manage the data and takes decision to what extent the personal data would communicate to others (Westin and Louis, 1970). In the literature review, Skinner identified privacy in three different levels – individual, group and organization. Societal level (Smith *et al.*, 2011) explained as one which is used for analysis in privacy concern within cross-cultural or across the nation. APCO macro

model (Smith *et al.*, 2011) "Antecedents => Privacy Concerns =>Outcomes", considered by examining the central construct "Privacy Concerns" (e.g. perception, beliefs), antecedents (privacy experiences, privacy awareness, demographic difference, culture), and then focus on the outcomes (regulations, behavioural reactions, trust, privacy calculus) and associated relationships.

The dimensions of information privacy

The privacy concern measures the degree of control by consumers (Fletcher and Peters, 1997) over the personally identifiable information. Milberg *et al.* (2000) explained in a study, which revealed that the privacy concern influences the attitude of individuals such as acceptance, willingness, preferences. It depends upon the individual perceptions to evaluate the correspondence of privacy concern by taking different dimensional factors (Van Slyke *et al.*, 2006). In the process of conceptualization of IPC, Hong and Thong (2013) identified six key dimensions, and those are errors, usage, improper access, collection, control and awareness. Fear is another dimension where one is browsing details can be monitored and captured (Dinev and Hart, 2004). If there is an advancement in technology, then inappropriate accessibility of personal information could have restricted, and it will limit the inappropriate access in public domain of all stakeholders. Personal information and identity issues, with the uncertainty of user identification over the internet are gathered using the collection dimension.

Researchers have also tried to explain other dimensions by focusing on instruments like CFIP – concern for information privacy and IUIPC - Internet user's data privacy concerns. The CFIP has focused on four dimensions includes data collection, error in data, unauthorized use of data and unauthorized access (Smith *et al.*, 1996). At a later stage, a new version of the internet user's information privacy concerns construct has evolved and focused on three main dimensions – collection mechanism, awareness and control (Malhotra *et al.*, 2004). The willingness of a person in a transaction varies in internet user's information privacy concerns instrument than concern for information privacy.

Theoretical contributions

There are theoretical contributions to information privacy research using from Gregor's (2006) designed framework concept, which classifies them into five different types – analysing, explaining, predicting, explaining and predicting and the last one is design and action (Gregor, 2006). First theory type describes the essence of information privacy, and it explains by analysing the necessity of its state. Second theory type explains details on information privacy research, and it does not contribute any expectations. Third theory type explains that it gives some concrete predictable results without developing real relationships. Fourth theory type explains both the testable results and explains the causal relationship between them. Fifth theory type explains the design and action type which specially designed tool for providing information privacy. Reagle and Cranor (1999) and Cranor *et al.* (2006) defined that each website has their own privacy protection protocol framework to define their own website related protection policy, and it matches with the user's privacy preferences. The tools would confirm them about their utilization of websites for the transaction, and it would assure them for safe use, and after then, this increases the behavioural trust of a consumer for the websites. Also, it could encourage consumers to measure the privacy attitude when transacting with a website.

The level of analysis in information privacy concerns

Skinner *et al.* (2006) identified individual, group and organizational as three levels of information privacy. After then, the article written by Smith *et al.* classified and described

four levels of privacy as an individual, group, organizational and societal. Most of the information privacy research conducted first at individual levels, and it has implications at other levels. In the second level analysis researcher conceptualized privacy as a multilevel concept, and it has identified research effect on the phenomenon occurring at or across multilevel occurrences concurrently. In some cases, researchers look at some point of interaction between individuals and organizational approaches (Miyazaki and Krishnamurthy, 2002); Milne and Gordon (1993) gave insight on IPC at individuals as well as to the societal level of analysis. Smith (2004) and Schwaig *et al.* (2005) gave on organizational approaches on social culture which give an insight of multilevel approaches, and it encourages further study of the multilevel concept. The key identifiers of different literatures are listed in the appendix of our study.

Researchers addressed the IPC in the lens of multilevel concept, on how customer needs to be achieved by fair information practice (FIP). Earp *et al.* (2005) identified that all the privacy policies are meet the objectives of company's viewpoint and not related from the customer's side. Few literatures confirm that only a limited number of the population read and understand the privacy policies (Meinert *et al.*, 2006) or people do not like or recognize privacy concern (Awad and Krishnan, 2006). To derive value from individual data and to make the balance between consumers for privacy protection and the desire for dealing business led to the design of FIP standards.

The classification of literature is based on the level of analysis and the area of research has been done so far. Table 2 summarizes (journal articles) that very limited research has been done on information privacy (IP) at different levels. Individual, group and organization are the levels of information privacy been classified and defined by Skinner *et al.* (2006). After then, Smith *et al.* (2011) uses four levels of analysis by adding a new societal level into the existing classification, and these levels are studied rigorously by following the previous research by Clark *et al.* (2007). In Table 2, it is found that information privacy been considered in various articles and few journal articles are found which counted more than one. Due to the availability of validated instruments, the individual level of study has been conducted sufficiently by collecting and analysing data from a huge number of individuals. Besides individual levels, we are not found sufficient literatures for other level of information privacy research. Table 2 reveals that several researches done at organizational level of study and that has been carried out in the area as information privacy practices. We have found that at the organizational level there are not much work has been done so far in IP research. With regards to e-business, organization always eager to know the impact of IP concern, which can influence a decisive achievement of the online business activity. We have found a very limited study has been done at group level IP research and researcher needs to focus more on these levels of study. Societal level is another level of approach where culture play a vital role in it. These approaches which give more in-depth information of different construct of privacy, and it varies differently in culture and various cultural values in different countries (Milberg *et al.*, 2000). It is better to understand the information privacy of citizens in a standardized way because of the exponential growing appeal towards the corporation and government from a worldwide crowd.

Table 2. Classification of literature on level of analysis

Level of analysis	Privacy	Information privacy concern (IPC)
Individual	29	10
Group	2	0
Organization	11	0
Societal	9	3

So, we cannot overlook the growing advent of societal effect in privacy research and researcher needs to give more attention towards the societal level of analysis. At societal level, it includes all the societal phenomenon with the group, organization and individuals in the IP level of analysis.

Individual level

The statement, right to be alone in the right to privacy, described as the right of a person to be alone by isolation from the attention of others (Warren and Brandeis, 1890). Information privacy as an option to secrecy by that everyone has the right to restrict the information about themselves in public and where outsiders should not be encouraged to take advantage of it (Posner, 1983). Privacy can be observed with autonomy (Kufer, 1987), a segment closely associated with personhood. Privacy and autonomy (Kufer, 1987), are segments closely associated with personhood. An independent self-concept explains oneself as a "purposeful, self-determining, responsible agent" and awareness of an individual to control the boundary and to control who may access and to what extent.

Personal privacy relates to each concern where it will be restricted to protect personal decorum. Information privacy is the relationship between technology and the individual's ownership of collection and sharing of data (Smith *et al.*, 2011). The individual's perceptions of privacy is identified using the multidimensional development theory (MDT)and develop the framework (Laufer and Wolfe, 1977). MDT focuses on the multidimensional concept – mainly environmental concept, interpersonal interactions, and self-development. France Belanger and Robert Crossler (Belanger and Crossler, 2011) explained in the first phase of the multilevel framework of I.S. research at the individual level. We have considered three areas of concern in this research, i.e.

(1) Attitude

Information privacy attitude refers to the individual perceptions and reactions to the information policies, practices and tools and technologies. Privacy attitude includes preparedness to provide private data (Dillon *et al.*, 2008). The main issues of privacy attitude are mentioned as each study conceptualizes the attitude differently, and some case it is focused towards privacy in general (Razzouk *et al.*, 2008). Cao and Everard (2008) explained attitude can be used as dependent variables and in some cases, privacy attitude can be independent variables that used for preserving influence on behaviours and capability of adaptation of new technology towards information sharing's (Alge *et al.*, 2006; Thiesse, 2007; Webster, 1998). There are some finding of the attitude toward the privacy concern is that transparent information practices to be established to organize and manage the data security, and it will be protected enough that people automatically shared information through online by the faith and trust attribute (Culnan and Armstrong, 1999).

(2) Practices

Information privacy practice refers to organizational as well as individual actions about the protection of privacy with various interdependent factors which affect such privacy practices (Belanger and Crossler, 2011). There is some information that falsifying personal data and forcing towards deleting unwanted work attributes comes under individual privacy practice (Chen and Rea, 2004). There are some factors which affect privacy practices, include the different types of websites viewed and the originality of a site (Hsu, 2006). Sometimes, people may not know the actual practices they should follow when they are surfing on internet sites (Klasnja *et al.*, 2009). Fair information practices (FIP) provide assessments to the policies that maintained in organizational practice. Jensen and Potts (2004) explained and

some corresponding literature reveals that some companies do not give appropriate information about their privacy protection policies. In this case, consumers are not in a good mood to share their private information due to the lack of privacy protection policies. Some companies do not have such a policy when they comply with fair information practice standard (Liu and Arnett, 2002; Ryker *et al.*, 2002).

(3) Technology

Information privacy tools and technologies (Belanger and Crossler, 2011) research refers to the use of technological advancement on the evaluation of information privacy in a different dimension. Information privacy tools and techniques deal with privacy threats. There is research on tools and technologies which organization used to follow to abstract the privacy information of customers through the utilization of spyware and adware (Dobosz *et al.*, 2006), to violate on consumers' information privacy, and trust is another factor which seals organizations (Moores and Dhillon, 2003) used to protect information privacy of consumers.

Group level

In groups, the privacy information shared among the group members and outside. Researchers have found certain factors which influence group performance when it comes to privacy concerns. The factors are trust, fears, willingness and faithfulness, which influence the group dynamics behaviour among the members of the group. Information privacy on group behaviour is different from users from one group to another. In a group, when a person is trying to interact, privacy is becoming a constraint for the person (Westin, 1968). Nov and Wattal (2009) explained how an individual shows interest when trying to disclose private information in different group cultures and characteristics. Individual within a group is a core component when taken for analysis (Morgeson and Hofmann, 1999), and different groups also consisting of specific structures, constructs and identity (Watson-Manheim and Belanger, 2002). Watson-Manheim and Belanger (2007) defined that how technologies can be enhanced within groups with privacy policies to curbed the communication within the groups. Floridi (2017) defined group dynamics is the external factor concern which represents different variables like group distribution, group significance, group cohesion or group characteristics like size. Loi and Christen (2019) introduced two concepts in group privacy. They explained what confidential information shared with the group members and restrict to outside members. Furthermore, they clarified the inferential privacy where it manages the derivations that can be made about a group of individuals characterized by highlight, common by all person in a group. They contend that inferential privacy is unpersuasive to both of individual or group.

Organizational level

In the case of an organization, its policy dictates how the data is maintained. Organizational privacy (Smith *et al.*, 1996) concern refers to the information which is confidential and not disclosed to the public. Government organizations, corporates and private societies are adopting various alternatives to maintain data confidentiality and keep data in a secret form and restricting to give access to unwanted purpose. Organizational privacy concerns mainly represented by organizational leaders. Organizational leaders have access permission to those sources of information where privacy concern of individual also linked (Belanger and Crossler, 2011). Those concerns mainly arise from management privacy practices and related policies.

Societal level

Human beings are social by nature, who cannot survive without social co-operation and other association. In a society, there are lots of online platforms available where people are engaging themselves to interact among themselves (Alashoor *et al.*, 2017). They execute the command themselves to share their personal information either knowingly or unknowingly. However, some users are not known such type of concern at all when such information shared at the public domain in a bounded society (Spottswood and Hancock, 2017; Black *et al.*, 2015). Researchers also find that critical dimensions like own willingness, ability, preferences and openness, which are related to privacy concern at individual levels (Belanger and Crossler, 2011). As government and corporations are appealing more on the public interface, and they should give proper attention in favour of citizen-centric culture, employees of organization and consumers about the privacy concern.

Issues/barriers in information privacy

The increase in sharing information may lead to, in some ways, breaches in privacy. The state of privacy (Hughes, 2012) defined in different types of barriers in privacy concern. They are mainly physical, behavioural and normative. Physical barriers are the touchable observation of personal assets which restrict access from others. Behavioural barriers are maintaining privacy while communicating verbally or non-verbally. Normative barriers present laws and social norms that limit a person from intruding into the private life of others. Privacy has largely one of the ethical, social and legal issues in this digital world (Culnan and Bies, 2003). *Angst* and Agarwal (2009) defined that due to the huge utilization of internet technology and gathering of personal information, there are new challenges come to picture and it leads to information privacy concern. Also, people expected higher government involvement concern (Dinev *et al.*, 2006a), but a weak relation in use of e-business and privacy concern are observed (Dinev *et al.*, 2006b). Some companies give accurate data related to privacy concerns, but some refuse to give private information to the government (Sydell, 2006). The questions arise why such distinct behaviour of two companies within the same specific country. Some cases, individuals and organizations become contradictory to each other with respect to privacy. For example, if we take e-commerce transactions where a consumer desired that his/her information is to be used only for the transactions what they opted for. But in reality, the personal information has been used by the e-commerce website without known to the consumers. In this case, consumers' behaviour becomes unrealistic and creating a conflicting nature towards the organization and raise concern to privacy.

Conclusion and future directions of our research

This paper has limited itself to studying a part of the available literature on privacy concern in an information system. A more detailed overview can examine the same by increasing the number of articles with the specific domain application model included in the review. Research needs to focus on whether privacy concern is more as generality across the globe, or it is concerned with specified cultural domain and researchers to provide more testable results. Information system researchers need to investigate more on privacy concern in different countries. Research can also focus on various countries, how organization and individual relate together for the concerns for information privacy. Investigation can focus on why information privacy policy and protection laws are different for different companies in the same country. Due to the increase in usage of information technology, it becomes a challenge for keeping the information update concerning the stakeholder's privacy and security concern and how it can be managed suitably.

Future research could be to find out the privacy attitude and privacy concerns for within and between organizations. It needs to extract, how the business model enhanced to measure the privacy. Future studies can be explored with wide range of diversity like age, gender, income rather to student centric data. Students are keener to open towards their data rather than a professional. How can this be relating to privacy that affect adverse to the study. Other types of organization beyond e-commerce sites, such as government organizations, need to be investigated to extend the study further on privacy policy, privacy policy and protection. A great deal of research has been covered the individual level of analysis of privacy concern. Group concern for information privacy is a potentially fascinating and fruitful area for future research. How and what types of designed tools can be used to protect the concern towards privacy in a group where all the members are communicating with each other. Researchers have tried little research on group, organizational and societal level analysis. A multilevel analysis approach will lead in future research to adhere better insight that how different level of analysis can be enhanced.

References

Alashoor, T., Han, S. and Joseph, R.C. (2017), "Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: an APCO model", *Communications of the Association for Information Systems*, Vol. 41 No. 4, pp. 62-96, doi: 10.17705/1cais.04104.

Alge, B.J., Ballinger, G.A., Tangirala, S. and Oakley, J.L. (2006), "Information privacy in organizations: empowering creative and extra-role performance", *Journal of Applied Psychology*, Vol. 91 No. 1, p. 221.

Amor, D. (2002), *Internet Future Strategies: how Pervasive Computing Will Change the World*, Prentice Hall Professional.

Angst, C.M. and Agarwal, R. (2009), "Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion", *MIS Quarterly*, Vol. 33 No. 2, pp. 339-370.

Awad, N.F. and Krishnan, M.S. (2006), "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization", *MIS Quarterly*, Vol. 30 No. 1, pp. 13-28.

Belanger, F. and Crossler, R.E. (2011), "Privacy in the digital age: a review of information privacy research in information systems", *MIS Quarterly*, Vol. 35 No. 4, pp. 1017-1041.

Belanger, F. and Hiller, J.S. (2006), "A framework for e-government: privacy implications", *Business Process Management Journal*, Vol. 12 No. 1, pp. 48-60.

Black, S.L., Stone, D.L. and Johnson, A.F. (2015), "Use of social networking websites on applicant's privacy", *Employee Responsibilities and Rights Journal*, Vol. 27 No. 2, pp. 115-159.

Brown, M. and Muchira, R. (2004), "Investigating the relationship between internet privacy concerns and online purchase behavior", *Journal of Electronic Commerce Research*, Vol. 5 No. 1, pp. 62-70.

Burton, S.H., Tanner, K.W., Giraud-Carrier, C.G., West, J.H. and Barnes, M.D. (2012), "Right time, right place health communication on Twitter: value and accuracy of location information", *Journal of Medical Internet Research*, Vol. 14 No. 6.

Cao, J. and Everard, A. (2008), "User attitude towards instant messaging: the effect of espoused national cultural values on awareness and privacy", *Journal of Global Information Technology Management*, Vol. 11 No. 2, pp. 30-57.

Chen, K. and Rea, A.I. (2004), "Protecting personal information online: a survey of user privacy concerns and control techniques", *Journal of Computer Information Systems*, Vol. 44 No. 4, pp. 85-92.

Clark, T.D. Jr., Jones, M.C. and Armstrong, C.P. (2007), "The dynamic structure of management support systems: theory development, research focus, and direction", *MIS Quarterly*, Vol. 31 No. 3, pp. 579-615.

Cranor, L.F., Guduru, P. and Arjula, M. (2006), "User interfaces for privacy agents", *ACM Transactions on Computer-Human Interaction*, Vol. 13 No. 2, pp. 135-178.

Culnan, M.J. and Armstrong, P.K. (1999), "Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation", *Organization Science*, Vol. 10 No. 1, pp. 104-115.

Culnan, M.J. and Bies, R.J. (2003), "Consumer privacy: balancing economic and justice considerations", *Journal of Social Issues*, Vol. 59 No. 2, pp. 323-342.

Culnan, M.J. and Williams, C.C. (2009), "How ethics can enhance organizational privacy: lessons from the choice point and TJX data breaches", *MIS Quarterly*, Vol. 33 No. 4, pp. 673-687.

Dillon, T.W., Hamilton, A.J., Thomas, D.S. and Usry, M.L. (2008), "The importance of communicating workplace privacy policies", *Employee Responsibilities and Rights Journal*, Vol. 20 No. 2, pp. 119-139.

Dinev, T. and Hart, P. (2004), "Internet privacy concerns and their antecedents – measurement validity and a regression model", *Behaviour and Information Technology*, Vol. 23 No. 6, pp. 413-423.

Dinev, T. and Hart, P. (2006), "An extended privacy calculus model for e-commerce transactions", *Information Systems Research*, Vol. 17 No. 1, pp. 61-80.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. (2006a), "Internet users' privacy concerns and beliefs about government surveillance: an exploratory study of differences between Italy and the United States", *Journal of Global Information Management*, Vol. 14 No. 4, pp. 57-93.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. (2006b), "Privacy calculus model in e-commerce – a study of Italy and the United States", *European Journal of Information Systems*, Vol. 15 No. 4, pp. 389-402.

Dobosz, B., Green, K. and Sisler, G. (2006), "Behavioral marketing: security and privacy issues", *Journal of Information Privacy and Security*, Vol. 2 No. 4, pp. 45-59.

Donaldson, T. and Dunfee, T.W. (1994), "Toward a unified conception of business ethics: integrative social contracts theory", *Academy of Management Review*, Vol. 19 No. 2, pp. 252-284.

Earp, J.B., Anton, A.I., Aiman-Smith, L. and Stufflebeam, W.H. (2005), "Examining internet privacy policies within the context of user privacy values", *IEEE Transactions on Engineering Management*, Vol. 52 No. 2, pp. 227-237.

Fletcher, K.P. and Peters, L.D. (1997), "Trust and direct marketing environments: a consumer perspective", *Journal of Marketing Management*, Vol. 13 No. 6, pp. 523-539.

Floridi, L. (2017), "Group privacy: a defence and an interpretation", *Group Privacy*, pp. 83-100.

Fried, C. (1968), "Privacy", *The Yale Law Journal*, Vol. 77 No. 3, pp. 475-493, doi: 10.2307/794941.

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M. and Pourzandi, M. (2012), "A quantitative analysis of current security concerns and solutions for cloud computing", *Journal of Cloud Computing: Advances, Systems and Applications*, Vol. 1 No. 1, p. 11.

Gregor, S. (2006), "The nature of theory in information systems", *MIS Quarterly*, Vol. 30 No. 3, pp. 611-642.

Hong, W. and Thong, J.Y.L. (2013), "Internet privacy concerns: an integrated conceptualization and four empirical studies", *MIS Quarterly*, Vol. 37 No. 1, pp. 275-298.

Hsu, C.W. (2006), "Privacy concerns, privacy practices, and website categories: toward a situational paradigm", *Online Information Review*, Vol. 30 No. 5, pp. 569-586.

Hughes, K. (2012), "A behavioural understanding of privacy and its implications for privacy law", *The Modern Law Review*, Vol. 75 No. 5, pp. 806-836.

Jensen, C. and Potts, C. (2004), "Privacy policies as decision-making tools: an evaluation of online privacy notices", *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pp. 471-478.

Jentzsch, N. (2001), "The economics and regulation of financial privacy: a comparative analysis of the United States and Europe", Working Paper, John F. Kennedy Institute.

Kharade, J. (2016), "G2C E-governance project implementation at local level in a Pune division context, BVIMSR's", *Journal of Management Research*, Vol. 8 No. 1, p. 19.

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B.M., LeGrand, L., Powledge, P. and Wetherall, D. (2009), "When I am on wi-fi, I am fearless: privacy concerns and practices in everyday wi-fi use", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1993-2002.

Kufer, J. (1987), "Privacy, autonomy, and self-concept", *American Philosophical Quarterly*, Vol. 24 No. 1, pp. 81-89.

Kyei-Blankson, L., Iyer, K.S. and Subramanian, L. (2016), "Social networking sites: college students' patterns of use and concerns for privacy and trust by gender, ethnicity, and employment status", *International Journal of Information and Communication Technology Education (IJICTE)*, Vol. 12 No. 4, pp. 62-75.

Laufer, R.S. and Wolfe, M. (1977), "Privacy as a concept and a social issue: a multidimensional development theory", *Journal of Social Issues*, Vol. 33 No. 3, pp. 22-42.

Li, X.B. and Sarkar, S. (2006), "Privacy protection in data mining: a perturbation approach for categorical data", *Information Systems Research*, Vol. 17 No. 3, pp. 254-270.

Liu, C. and Arnett, K.P. (2002), "Raising a red flag on global WWW privacy policies", *Journal of Computer Information Systems*, Vol. 43 No. 1, pp. 117-127.

Loi, M. and Christen, M. (2019), "Two concepts of group privacy", *Philosophy and Technology*, Vol. 33 No. 2, pp. 1-18.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research*, Vol. 15 No. 4, pp. 336-355.

Martin, K. (2016), "Do privacy notices matter? Comparing the impact of violating formal privacy notices and informal privacy norms on consumer trust online", *The Journal of Legal Studies*, Vol. 45, pp. S191-S215.

Meinert, D.B., Peterson, D.K., Criswell, J.R. and Crossland, M.D. (2006), "Privacy policy statements and consumer willingness to provide personal information", *Journal of Electronic Commerce in Organizations*, Vol. 4 No. 1, pp. 1-17.

Milberg, S.J., Smith, H.J. and Burke, S.J. (2000), "Information privacy: corporate management and national regulation", *Organization Science*, Vol. 11 No. 1, pp. 35-57.

Milne, G.R. and Gordon, M.E. (1993), "Direct mail privacy-efficiency trade-offs within an implied social contract framework", *Journal of Public Policy and Marketing*, Vol. 12 No. 2, pp. 206-215.

Miyazaki, A.D. and Krishnamurthy, S. (2002), "Internet seals of approval: effects of online privacy policies and consumer perceptions", *Journal of Consumer Affairs*, Vol. 36 No. 1, pp. 28-49.

Moores, T.T. and Dhillon, G. (2003), "Do privacy seals in e-commerce really work?", *Communications of the ACM*, Vol. 46 No. 12, pp. 265-271.

Morgeson, F.P. and Hofmann, D.A. (1999), "The structure and function of collective constructs: implications for multilevel research and theory development", *Academy of Management*, Vol. 24 No. 2, pp. 249-265.

Norberg, P.A. and Horne, D.R. (2007), "Privacy attitudes and privacy-related behavior", *Psychology and Marketing*, Vol. 24 No. 10, pp. 829-847.

Normalini, M.K. and Ramayah, T. (2017), "Trust in internet banking in Malaysia and the moderating influence of perceived effectiveness of biometrics technology on perceived privacy and security", *Journal of Management Sciences*, Vol. 4 No. 1, pp. 3-26.

Nov, O. and Wattal, S. (2009), "Social computing privacy concerns: antecedents and effects", *Proceedings of the 27th International Conference on Human Factors in Computing Systems*, Boston, MA, April 4-9, pp. 333-336.

Omariba, Z.B., Masese, N.B. and Wanyembi, G. (2012), "Security and privacy of electronic banking", *International Journal of Computer Science Issues*, Vol. 9 No. 3, pp. 432-446.

Ovengalt, C.T., Djouani, K., Kurien, A.M. and Chibani, A. (2017), "A context broker for better access to quality and cost-effective healthcare", *Procedia Computer Science*, Vol. 109, pp. 988-993.

Posner, R.A. (1983), *The Economics of Justice (5. print ed.)*, Harvard University Press. Cambridge, MA, p. 271.

Raval, D. and Jangale, S. (2016), "Cloud-based information security and privacy in healthcare", *International Journal of Computer Applications*, Vol. 150 No. 4.

Razzouk, N.Y., Seitz, V. and Nicolaou, M. (2008), "Consumer concerns regarding RFID privacy: an empirical study", *Journal of Global Business and Technology*, Vol. 4 No. 1, p. 69.

Reagle, J. and Cranor, L.F. (1999), "The platform for privacy preferences", *Communications of the Acm*, Vol. 42 No. 2, pp. 48-51.

Ryker, R., Lafleur, E., McManis, B. and Cox, K.C. (2002), "Online privacy policies: an assessment of the Fortune E-50", *Journal of Computer Information Systems*, Vol. 42 No. 4, pp. 15-20.

Saha, S., Bhattacharyya, D., Kim, T.H. and Bandyopadhyay, S.K. (2010), "Model-based threat and vulnerability analysis of e-governance systems", *International Journal of U-& E-Service, Science and Technology*, Vol. 3 No. 2, pp. 7-21.

Schwaig, K.S., Kane, G.C. and Storey, V.C. (2005), "Privacy, fair information practices and the fortune 500: the virtual reality of compliance", *Acm Sigmis Database: The Database for Advances in Information Systems*, Vol. 36 No. 1, pp. 49-63.

Singh, A.J. and Chauhan, R. (2012), "Technology challenges in e-service accessibility", *Journal of Engineering and Technology*, Vol. 2 No. 1, p. 32.

Skinner, G., Han, S. and Chang, E. (2006), "An information privacy taxonomy for collaborative environments", *Information Management and Computer Security*, Vol. 14 No. 4, pp. 382-394.

Smith, H.J. (2004), "Information privacy and its management", *MIS Quarterly Executive*, Vol. 3 No. 4, pp. 291-313.

Smith, H.J., Dinev, T. and Xu, H. (2011), "Information privacy research: an interdisciplinary review", *MIS Quarterly*, Vol. 35 No. 4, pp. 989-1016.

Smith, H.J., Milberg, S.J. and Burke, S.J. (1996), "Information privacy: measuring individuals' concerns about organizational practices", *MIS Quarterly*, Vol. 20 No. 2, pp. 167-196.

Sohail, M.S. and Al-Jabri, I.M. (2014), "Attitudes towards mobile banking: are there any differences between users and non-users?", *Behavior and Information Technology*, Vol. 33 No. 4, pp. 335-344.

Spottswood, E.L. and Hancock, J.T. (2017), "Should I share that? Promoting social norms that influence privacy behaviors on a social networking Site", *Journal of Computer-Mediated Communication*, Vol. 22 No. 2, pp. 55-70.

Straub, D.W., Jr and Collins, R.W. (1990), "Key information liability issues facing managers: software piracy, proprietary databases, and individual rights to privacy", *MIS Quarterly*, Vol. 14 No. 2, pp. 143-156.

Swani, K. and Brown, B.P. (2011), "The effectiveness of social media messages in organizational buying contexts", *American Marketing Association*, Vol. 22, p. 519.

Sydell, L. (2006), "Google fights request to turn over search records", NPR, January 20, available at: www.npr.org/templates/story/story.php?storyId=5165530

Tham, R., Buykx, P., Kinsman, L., Ward, B., Humphreys, J.S., Asaid, A., Tuohey, K. and Jenner, R. (2014), "Staff perceptions of primary healthcare service change: influences on staff satisfaction", *Australian Health Review*, Vol. 38 No. 5, pp. 580-583.

Thiesse, F. (2007), "RFID, privacy and the perception of risk: a strategic framework", *The Journal of Strategic Information Systems*, Vol. 16 No. 2, pp. 214-232.

Van Slyke, C., Shim, J.T., Johnson, R. and Jiang, J. (2006), "Concern for information privacy and online consumer purchasing", *Journal of the Association for Information Systems*, Vol. 7 No. 6, pp. 415-444.

Warren, S.D. and Brandeis, L.D. (1890), "The right to privacy", *Harvard Law Review*, Vol. 4 No. 5, pp. 193-220.

Watson-Manheim, M.B. and Belanger, F. (2002), "Support for communication-based work processes in virtual work", *E-Service Journal*, Vol. 1 No. 3, pp. 61-82.

Watson-Manheim, M.B. and Belanger, F. (2007), "Communication media repertoires: dealing with the multiplicity of media choices", *MIS Quarterly*, Vol. 31 No. 2, pp. 267-293.

Webster, J. (1998), "Desktop video conferencing: experiences of complete users, wary users, and non-users", *MIS Quarterly*, Vol. 22 No. 3, pp. 257-286.

Westin, A.F. (1968), "Privacy and freedom", *Washington and Lee Law Review*, Vol. 25 No. 1, p. 166.

Westin, A.F. and Louis, B.-C. (1970), *Privacy and Freedom*, Bodley Head, London, ISBN 978-0370013251, p. 7.

Yadav, D.S. (2006), *Foundations of Information Technology*, New Age International.

Further reading

Chen, S. and Li, J. (2009), "Factors influencing the consumers' willingness to buy in e-Commerce", *Proceedings of the International Conference on E-Business and Information System Security*, Wuhan, May 23-24, pp. 1-8.

Floridi, L. (2014), "Open data, data protection, and group privacy", *Philosophy and Technology*, Vol. 27 No. 1, pp. 1-3.

Razavi, M.N. and Iverson, L. (2006), "A grounded theory of information sharing behavior in a personal learning space", *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, Banff, Alberta, November 4-8, pp. 459-468.

Corresponding author

Ajit Kumar can be contacted at: ajit@ximb.ac.in