TITLE : INFORMATION PRIVACY AND SURVEILLANCE: A STUDY OF THE USE OF DIGITAL MEDIA BY THE CONSUMER

Authors:

Dr. Kapou Malakar[1], Assistant Professor, Department of Mass Communication and Journalism, Tezpur University, Email id: kapoumalakar@gmail.com, Phone: 9401498071

Rizwan Choudhury[2], M.A., Department of Mass Communication and Journalism, Tezpur University

Abstract

The right to privacy is an issue of greater in scope and effects in today's world considering the massive technological advancements. From the perspective of the consumer who uses the handheld mobile technology aggressively in this growing world of speed and communication, the right to privacy is a major concern which is often expressed in many forms but often not attended in our country as seriously as in other countries.

The study attempts to find out the level of the awareness about the issue of privacy among youth. The research throws upon light on the various opinions endorsed by the Government, UN and other international bodies. The study assesses the existing legal provisions on information privacy and concluded with the interpretation of the consumer's perspective with recommendations on how the issues could be dealt in the coming future.

Keywords: *Information Privacy, Surveillance Technologies, Internet and Privacy, Consumer's privacy*

Introduction

The 21st century has seen a growing number of ways to use information as almost all individual activities involve some kind of data transmission or another. With the initiative of Government of India on Digital India Projectto bring change in information processing in all sectors of the society, India has too entered into this digital revolution. This has resulted in the inevitability of data collection process with the shift to digital economy.The Internet has made collecting, organizing and handling personal data, directly or indirectly a key part of existing business model.

The dichotomy involves when information or data is required for many benefits which is to be indirectly percolated to society. This raises concerns because of arbitrary and unregulated use of data,

especially personal data of individual and consumers of apps that further interfere in the privacy and autonomy of the individual. Privacy is considered to be a right that fall under personal liberty of the individual. The Supreme Court of India in a landmark judgement on 24thAugust, 2017, recognized the right to privacy as a fundamental right protected under part III of the constitution of India

The right to privacy is being recognised as a human right by the United Nation Organization under Article 12 of the 1948, The Universal Declaration of Human Rights. Different dimensions of privacy outlined as human rights by UN declaration of human rights comprise privacy of an individual, the personal behaviour of the individual, the personal communication and the transfer of personal data of the individual concerned.

However, there is no precise definition of right to privacy. Available literatures mention the dual aspects of Privacy. First, the privacy is a human right. It is the liberty of the person to decide what he or she wants to keep private or public. Secondly, it is concerned with personal data or information, the extent to which an individual allows his/her personal data/information to be shared with other parties or the extent to which the privacy of the individual can be intruded by the state or government. Personal data involves email addresses, addresses of residence, face data, location data, activity log. There are variety of online data extraction system such as cloud storage, geolocation, biometric information, always aware assistants, speech recognition, personal chats, search history and so on.

Other nuances involve when there is an increasing surveillance of government without having any data protection regime. In India there is no comprehensive set of privacy rights/principles addressing data use, collection, and disclosure. In the digital era, information privacy and surveillance has been an emerging area of concern which is directly and indirectly related to various form of cybercrimes, scam and phishing. On the other hand, mass surveillance can hinder the larger democratic process and also impact human and personal rights including those affecting personal integrity.

The understanding of privacy has been shaped by the available technologies at consumer's end. Privacy and security concerns and trust and beliefs of the individual affect the risk perception of the consumers. The study area falls in the awareness of privacy rights of the consumers while consuming or using the digital media applications.

It is an effort to study the privacy behaviour of Individuals who have no understanding of the actual privacy threats in the online world and are unaware of the amount of personally identifiable information they have given to an infinite number of people. Data security is becoming increasingly crucial in recent years, especially because so many services have been moved to the digital sphere who are often asked to provide their data while they log in for online services and make purchases.

Rise of Digital Media and Consumer's Privacy

Digital media has come a long way in a few years and it continues to expand.Dictionary definition of digital media refers to conversion of analogue data to digital data. The Internet, a digital media is a huge global infrastructure connecting computer networks. With newer version of web, a range of websites and applications emerge out and allow to build and distribute online content or materials, making the everyday transactions easier. These apps range from home automation to e-commerce to ride hailing services and more. The benefits of the advancement of technology enables people to develop, share, cooperate and connect. Two significant development have made information privacy more stringent, e.g. 1) transition from websites to apps when delivering digital services, 2) mushrooming of smart devices which put millions of mobile applications at the user's fingertips.
Social Networking Site has created new interest groups and communities and given the opportunities to share latest news and views. The emerging trend of connecting people has further raised sensitive issues with the possible susceptibility of counterfeited private information.

With the advent of Internet and gradual developments in surveillance technologies as employed in collecting and retaining mass of information from users and consumers, the concern for privacy has been growing in the modern world. The discourse around privacy represents the way third party handles the information transacted in the online in the wake of omnipresence of personal data. The discourse of privacy is further connected to the security and protection of information of consumer of the technology, the capacity and motivation to access the services via digital technologies and apps, the corresponding mental state and environmental condition in the uses of a technology. Risk dimension of privacy is often known as the intimacy risk which concerns how e shops/e commerce companies use data for own interest, sell the customer database to third parties and expose consumers to unwarranted advertising messages. Some literature (Christian L, Van Tonder 2003; Dhouha Jaziri, 2014) mentioned about postmodern consumers, when consumption provides a meaning to life and add more value to life. The values, as articulated by these studies which the consumer realize may be utilitarian, hedonic, practical or momentary. The consumption is an engaging psychological, emotional and physical commotion that involves the consumer in picking out, acquiring and using, disposing of goods and services so as to gratify needs and desires.

India is the leading consumer of information in the world today. The rate of internet data is relatively lower and competitive compared to other markets in the world. "According to Mobile Broadband India Traffic (MBiT) Index formulated by Nokia Data consumption in India has grown by 47% in 2019 with 4G constituting 96% of the total data traffic consumed across the country"(The Economic Times Report, Feb 27, 2020).With the advent of 4G mobile communication technology and heavy

competition in the data and smartphone market by key players in the country, the accessibility to use of data has been much easier than before. The easy availability with no charges of many newer applications online has parallelly boosted the uses of the same in mobile phones and social media platforms.

India has been the emerging business destination of health and tourism sector and with low investment cost India has already impelled India to become the hub for Business process outsourcing. BPO, comprises a larger part of IT industry, many of which are concerned about their data compliance necessities in India. Many international E commerce Industries follow the guidelines ofDataProtection Act 1998 and Electronic Communications Privacy Act of 1986 in USA regarding the cyber challenges. Regarding data protection legal directives and principles EU, OECD have attempted address the issue of data protection of E commerce, BPOs and IT industries at the international level.

However, in the absence of any sound legal framework in India, many BPOs approach to ISO and ITEL in dealing with data transfer and data security. Many BPOs use the ISMS (Information Security Management System) for the protection of data and information processed.

Surveillance Framework in India

Surveillance refers to close observation of a suspected person or group. With arrays of government technologies in place,Government of India has adopted various surveillance technologies with a pursuit tocontrol and prevent untoward actions by monitoring public and private spaces of inhabitants. The pervasive nature of surveillance intends to invade into personal space of the individual, track the behaviour and activities of Individuals by calculating and analysing countless information collected via employed surveillance technologies.

The older statute e.g. Indian Telegraph Act (1885) has been one important legal jurisprudence on surveillance in India originated in the context of interception of telecommunication messages. Another statues that come under the current surveillance framework in India is electronic surveillance under the 2000 Information Technology Act (Bhatia, 2018).

An article of Mardev Jain (2019) mentions the shortcomings in security of AADHAR. The AADHAR is one of the world's largest biometric database project initiated in India with approximately 1.2 billion registrations, covering around 89 % of India's population. the Government of India can access to the information of citizens, track the activities of suspicious individuals through their Aadhaar number, which will link them to other services the citizens use. The process of obtaining the 'Aadhaar Card' involves the collection of fingerprints of citizens, retina scans as well as their face photos.

One of Aadhaar's main criticisms has been the numerous major security lapses that have been ubiquitous in Aadhaar 's operation, which have made the system prone to data leakage. UIDIA, Unique Identification Authority of India, has been shut down, on a regular basis, sometimes fraudulent websites keep popping up, disguising themselves as official websites, and phishing people for their personal information.

The contradictoryaspect of surveillance lies in the various push programs of government which are being carried out to scan citizens' activities and patterns and inevitablylabelsome people as dangerous anddistrustful. However, this may help to combat crime and control terrorism, which has the potential to turn India into an oppressive surveillance state.

Contextualizing Privacy

The dictionary definition of privacy states, "*the state of being alone and not watched or interrupted by other people*", "*the state of being free from the attention of the public*" (oxford dictionary).

Irwin Altman (1975) in his book described about three aspects of privacy. The first aspects is spatial privacy or physical space which represents private versus public space to what extent an individual's territorial privacy is protected from intrusion of others. Intrusion of physical space can be viewed when, for example, telemarketing calls, unwanted ads keep on disturbing one's privacy. The second aspects of privacy representsa person'scapacity to make certain choices without any intrusion or interference. The third aspect of privacy deals with the information privacy. The information privacy is concerned with individual's control over the flow of personal information across various platforms e.g., the practice of procurement, informationleak or disclosure, and further use. This strand of privacy is conquered when, for example, someone obtains sensitive personal data by digging confidential files without permission(Irwin, 1975).

On the other hand, both the terms, data privacy and data protection are alternatively used which can be briefly defined as information privacy, an aspect of information technology (IT). Data privacyaddresses ability of a formal or information organization or and individual to govern the merging and sharing of information via computer system with third parties. The Internet has introduced both new markets and business model for those who consider and practice information collection, organization and distribution, explicitly as a vital component of their businesses. Whereas information can be utilized for useful purpose, the unregulated and subjective use of personal information has raised concerns with respect to the intrusion of privacy and independence of a person.

Literature Review

As an attempt to grasp the views of consumers and how they value their private information or data given in the current scenario, the study reviews the existing laws and writings that are concerned with the privacy of individual, some current trends in the policies on Privacy and Surveillance.

In one longstanding literature, the author, Westin defines (1967) information privacy, "As the individual's ability to control the conditions under which his/her personal information is collected and used."

Kim, Malhotra and Agarwal (2004) in their study stress on the three dimensions of information privacy broadly collection, control and awareness. Collection represents the level of concern of individual about the sum of personal information possessed by third parties, in comparison with the benefits received by individual over the submission of personal data. Control is defined as the ability of consumers to be aware of submitted personal information, access and use the personal data or information, delete and change of it. Awareness is defined as the level of individual awareness or consciousness about the privacy practices of the company.

In another study, carried out by Burke Smith and Milberg, (1996) mentioned about other two dimensions of unauthorized use of personal information. The first one refers to secondary internal use which represents the use of collected information for a specific purpose by an organization/company without the consent of the individual.
Unauthorized secondary external use focusses on the collection of information for a specific purpose which can be used for another purpose once it is shared and exposed to an outside organization.

On the contrary, Eggert, (2006) demonstrates that higher level of privacy concern reduces the consumer's trust on online platforms and heightens the level of perceived risk of online transaction. He argues that trust reduces perceived doubt and perceived helplessness of users when they consume a service online.

The study of Zhang et al, (1992) finds that privacy concern while shopping online decreases the level of pleasure of the consumers which they obtain from shopping. The shopping is considered as an intrinsic impetus which propels individual to sacrifice their information privacy in order to get their consuming disposition satisfied. Increasing level of privacy concerns might lead to psychological burden on consumers.

Review of Existing Legal Instrument on Privacy

The Information Technology Act (ITA) 2000 involves gamut of provisions that reassess the right to privacy of individual in electronic platforms. Protection of privacy rights has been ensured in view of cybercrimes e.g. hacking, child pornography, cyber fraud etc while safeguardingand penalizing the same. However, ITA does not address certain questions and circumstances like information flows across the databases, the evidentiary status of content in social media in India,merging and sharing of data or information, the user's right to be notified of the presence of do-not-track options and cookiesand the users' right to inquire the service providers for taking down and deleting their personal content.

The ITA while reinforced the privacy rights of the individual and body corporate, comprehend the necessity of having "reasonable security practices and actions for sensitive personal data or information". The ITA rules make the body corporate obliged to maintain the privacy of consumer's information. The rules further ensure the right of the individual over their personal information.

The Information Technology Act (ITA) 2000 added further, " It is requires that any corporate body must publish an online privacy policy, provide individuals with the right to access and correct their information, obtain consent before disclosing sensitive personal information except in the case of law enforcement, provide individuals with the ability to withdraw consent, establish a grievance officer, require companies to ensure equivalent levels of protection when transferring information, and put in place reasonable security practices."

On the other hand, the Personal Data Protection Bill 2018, in India is being criticized for providing blanket authority to government to access data from citizens. Justice BN Srikrishna said in a media report (The Economic Times, July 2018) about the dangerous implications of the privacy bill which could turn India into an "Orwellian state". Justice BN Srikrishna led the committee that presented the report on the basis of which the original Bill was drafted in 2018(Bureau, 2018).

The bill seems to provide more sanction to the central government. The Section 35 of the bill allows government agency to bypass the interest of India 's sovereignty and integrity, state security, friendly relations with foreign states or public order and grant authority to prevent any recognizable offence in relation to the above.

On the other hand, The Personal Data Protection Bill intends to give individuals the right to access and correct data, the right to data portability which ensure the safeguard to users against their personal information get collected and hoard in silos or closed platforms.

The bill makes it easier for the individuals to reuse data or information for own purposes and reproduce and transfer the personal information from one environment to another in a safe and secured way without affecting its usability.

The Bill grants individual to get the personal data deleted if there is no legitimate reason to keep the data.

In contrast to this, the draft bill, 2018 comprises a few provisions for privacy protection of individual. Section 42 of the draft bill grants immunities to the central government for the singular purpose of 'state security'. The bills reinforces , "the processing of personal data will not be permitted unless the state is authorized in accordance with the law and in accordance with the procedure laid down by the law."

On the other hand, the bill 2019 stipulated more emphasize on a parliamentary law which is to be framed for the purpose of testing what is "necessary" or "proportionate" to the goals being sought to infringe privacy.

Certain statutory instruments that grant ancillary support to privacy in India includes Indian Telegraph Act, Indian Penal Code, Indian Contract Act 1872, Indian Copyright Act, Consumer Protection Act 1986, Specific Relief Act 1963 besides IT act and article 21 of the Indian constitution.

Research Methodology

The study aims to identify and assess the nuances involved in the right to individual privacy for consumers in using digital media in reference to the evolving marketing logic of the organizations/ companies in storing and sharing the information and growing numbers of innovative attempts of the government to put surveillance on citizens with the help of new apps and technologies.

Objectives

1. To study the perception of consumers about information privacy and surveillance while consuming arrays of digital apps in social media
2. To assess the level of awareness of consumers regarding information privacy associated with the digital media applications and services.
3. To study how do the existing laws and regulations describe the dichotomy between right to privacy of consumer and data collection prerequisites for service providers and application-software companies

The research setting is in India restricted within the demographic profile of age 18-30 of the population of 50 consumers.

An online survey is carried out toinquire about the level of awareness among consumers of apps about the data protection laws, as to how they view their personal data privacy, what level of monitoring by government they support. What motivates consumers to use apps? Can it be considered as the conscious submission of personal data and biometric data by consumers to various service providers, other agencies and government. The study comprises the choice and attitudes of the consumer about how they value their privacy.

Awareness of the Consumer: Choices and Attitudes

The awareness of the consumer is affected by the gratification of uses of social media. There are intrinsic motivations among consumers to become active media consumers. The sociability of social media that is derived from social integrative needs and tension-release needs assume more relevance than getting themselves aware about the privacy laws associated with an app. It is found that the way consumers perceive various virtues and attributes of social media technology affects their privacy concern when they use digital apps in social media. In certain circumstances, consumption of services is presumed to be so overwhelming and irresistible that the privacy concern becomes less important to consumer because the consuming needs and subsequent gratification they receive from the services subside the vices of the technology andthe application used. Hence, the attributes of connectivity and sociability of digital media count to be more dominant for consumers rather than their concern for snooping of privacy.

For young people today, it is a normal and integral part of everyday life to communicate online and to engage with others. When people log on, talk or engage in online social networks, the Internet is no longer just a resource, but an extension of their public identities and social lives. Although it is found that respondents are aware of the potential threats resulting from internet practices, such as malicious hacking, few appreciate the number of possible risks associated with sharing too much personal information online. However, most of the respondents are not aware that information can remain in cyberspace virtually forever and that can be viewed, copied and downloaded by anybody. As a result of which, the personal details that they share today can be used to humiliate, offend or defame them at a later date.

Likewise, the online activities of the respondents may be used secretly for marketing or commercial purposes. Perceptions of privacy are socially created by interaction and transactions with social entities in a connected society, a process that involves a certain degree of technological skills and digital literacy. The study finds that the knowledge and Internet literacy are also linked to both the information privacy of the Internet and the resultant usage by consumers. The respondents are asked if they read the “Terms & Conditions” of uses of one service online, before giving consent and agree to

Terms & Conditions, as they are only a click away from sharing their personal information, many say that they lack interest in reading.

Many consumers are not informed about what the act of sharing data truly means and how far consent of consumers is pertinent in case of information privacy.

The consumer respondents are asked if they read the privacy policy before using any internet-based apps or services. While 51 % are not sure, only 33.3 % are sure about it and the rest 15.7 % admit of not reading the privacy policy while transacting online and using any web based app or services. One third of the total respondents say that they read the policies to an extent. This gives an overall idea about the subconscious situation of a user, the way he or she pays importance to privacy vs information and entertainment through apps and websites. This helps to relate relevance of privacy for a person when it comes to sharing their personal information to the service providers or vendors.

Users when agree to user experience improvement programs on the personal devices are susceptible to provide access to data on pattern of usage behaviour and browsing history which is possible through search analytics. Applications like active voice recognition services assist the smart devices. The data are stored and curated with the help of artificial intelligence and machine learning, so as to provide the users better targeted ads and contents that are supposed to suit their likeness. Specific algorithms that help to manage these data, thus perform the desired task.

Other forms of data that may be collected from users when given permissions are personal information like location, email addresses, contact information and so on. Users knowingly or unknowingly give permission or agree to give access to personal information to the desired software provider, who, later, take it as a prerogative to regularly collect information either on device or on cloud to serve various purposes. Users provide personal data to software companies through user complaints and feedbacks and by agreeing to use the improved version of certain software programmes or software service products.

90% of respondents admit to have given permission to certain apps that collect personal information for addressing issues and bugs and providing a better user experience. While nearly 70 % of the total respondents admit to have given up personal information for improving user experience services. Only 40 % of them do read the terms and conditions involved for verifying such information.

The respondents are asked about enabling their microphone and location services for apps that they often use. Apps like MIUI community, mAadhar, MyJio etc often use location and microphone of the consumers even if these subsidiary features are not connected to the basic services provided to consumers . These are just a few examples, thus the users are asked if they either allow or notice their consuming pattern. About 17 % say they do often allow while 45 % occasionally allow the apps to take subsidiary information. When asked why do they allow, it is found that they allow because the

service matters the most for them than the surveillance. The respondents do not care much about the privacy right and believes more in consuming a service.

29.4 % are seriously concerned about their personal privacy online and 35.3 % are somewhat concerned and aware of privacy online. Aggregate of 64 %do care about their privacy which is not a low figure in terms of the consumer's consciousness of information privacy.

Perception of Consumers about Information Privacy and Surveillance

The privacy is connected to the dignity of the individual. The loss of control of one's own personal details is equivalent to losing control of one's existence and thus one's integrity. It is evident that respect for oneself is an end in itself rather than as a means and as an autonomous being, one demands for respect of one's privacy. Minimizing privacy also results in one becoming restricted and deprived the space to grow, experiment with oneself in the society. One loses his or her freedom of belief, free expression and freedom of information without privacy. Hence, the collection of information by mass surveillance is considered not only dangerous , but also has an effect on privacy regardless of whether or not the information is actually used.

In response to the awareness on the prevailing laws about data protection, privacy and surveillance that lie within the constitutional framework, only 47 % respondents respond positively. While 76 % of the respondents do seem to believe the fact that their data is available at the disposal for being used by the government whenever necessary for national or internal security purpose. 80 % of the respondents admit that they feel it is ethically or morally wrong to be tracked or kept under silent surveillance for security purposes without their consent or knowledge. 94 % respondents believe that the issue of Data Protection and Online surveillance should be addressed more crucially in the country.

60 % of the respondents feel the need for more apt and defined laws for addressing the matter of mass surveillance and data protection. Only 47 % believe that data privacy is a fundamental right, while right to privacy and right to data privacy do share some of the realms but they eventually aren't the same.

The respondents are asked if they are familiar with the existing and other legal instruments via IT act, that are available on privacy and surveillance. Prior Knowledge about available legal instruments establishes the fact that the respondents possess some idea about data protection policy framework or at least have heard about it. As seen from the feedback, nearly 51% of the respondents have no idea about the any privacy based legislation including IT actwhile the 49 % have heard about it. However, 27.1% of the total respondent admit that they are informed about the Personal Data Protection Bill 2018. India.

Critical Review of the Instruments of Privacy and Data Protection

Data privacy and data protection underlines onthe importance of safeguard of the personalsensitive information against breaches, unintendeddamage or deliberate loss and any form of cyber-attacks. Whereas data privacy emphasizes on guidelines on how companies can obtain, accumulate and process personal information, data protection focuses on security measures that ensure confidentiality, transparency and information availability.

Addressing privacy issues and safeguarding data privacy rights of the individual is a matter of global concern. There is no single law that can determine the right to privacy and data protection across the world. Apart from significant advances in data protection regime in European Union in the form of General Data Protection Regulation (GDPR), many countries like India, Brazil and New Zealand, have put respective privacy legislation in place and strengthen the existing laws to regulate the collection, storage, uses, discloser and transmission of personal data.

There is no mention about the rights of data subject, accountability of the service providers or companies to the consumer in GDPR. No detail account has been mentioned about cross border data transfer. In the floating demands of information and communication, transparency of information collected, processed and stored comprise vital part of right of privacy of individual (Krishnan, 2018). Yet, there is no reflection in GDPR about avenues that a country requires to focus upon like training and awareness regarding how consumer can receive the data breach notification. While data processing is a major area of concern, the notice to consumers about the uses of data and their subsequent consent is another important area missed out in GDPR.

The Personal Data Protection Bill is envisaged to instil a substantial impact on how consumer data is protected and kept private. With the growing awareness of privacy, consumers of digital apps and gadgets are expected to make more informed choices. The informed consumers are expected to make informed choice regarding certain brands and its associated services and exercise better options to dispense and reach more privacy controls.

Conclusion

The significance of privacy which is an important right to liberty which has been susceptible to intrusion directly and indirectly by the state in this digital age, cannot go unnoticed.

Consumers are willing to compromise for services or benefits which make them active participants of digital economy of sharing. As long as therisk does not seem great, consumers will keep on sharing their data. Many consumers do not read consent form or privacy notice with an attitude that they don’t trust the internet that it can safeguard their interest.

The Government's data protection policy must not deter the scope for the growth of the digital economy to the extent that it does not affect the privacy of personal data. Surveillance is essential to ensure the national security and enforcement of law with a mechanism of protection for the target of surveillance in place so that the technology becomes a facilitator instead of impediment. The recognition of the right to privacy as public interest provides an useful way to frame the surveillance debate. It affirms the need to reflect on mechanisms of supervision and transparency, bearing in mind the impact of unrestrained surveillance on the health of our democracy.

The world is increasingly digitalised with free flow online personal data. Although certain information are dear to all like birth date, personal chats or perhaps even financial data, then, people never cease to communicate in the online world considering the violation of privacy and potential misuse of data. Average users don't not bother how various services work around to secure internet data, although there is a major concern that information may be stolen and potentially misused. A few service providers are using our information to target ads, while miscreants are using it for pay. For a regular internet user, it is difficult to distinguish between the two types as it often lies in intent of the service provides. As long as users are connected to the online world, whether via a smartphone or a computer, data remains as sensitive as ever. End users are often very quick to hold the company accountable for not ensuring the security of our data each time a bug is discovered.

It is required for the Government of India to give attention to the matter of data protection with increasing public concerns, thus, ensure the enactment of data protection laws.It is essential to design a data collection policy that can sanction and appoint deliberate agencies with authority to collect the personal information. It is also required to make the purpose of collecting information visible for the individual consumers or users concerned.

The Right to Information (RTI) encourages the revelation of public information when it is asked for. It is essential to put in place a mechanism that would classify public, private and sensitive information so that it won't instigate the encroachment of personal information.

In the wake of newly emerging digital platforms and applications, it is essential on the part of individual to know about the collected information online via apps, website by the third parties, what kinds of information is being collected and its uses and if the collected information is shared or sold to others.Phones, computers and network drives, various encrypted softwareshould be required to have sufficient security checks in place. Government and the data protection commission must carry out awareness programme to target consumers through videos, messages, posters and other interactive sessions. When it comes to data privacy, it is important what people knows than how many people knows.

References

Book

- Irwin Altman, (1975) “The Environment and Social Behaviour: Privacy, Personal Space, Territory, Crowding” 146-51
- Westin, A. (1967). Privacy and freedom. New York: Atheneum.
- Blumler, J. G., & Katz, E. (1974). The Uses of mass communications: Current perspectives on gratifications research. Beverly Hills: Sage Publications.

Journal

- Malhotra, N., Kim,S.,& Agarwal, J.(2004).Internet user’s information privacy concerns (IUIPC):The construct the scale, and a causal model. Information Systems Research, 15(4), 336–355.
- Smith, H., Milberg, S., &Burke,S.(1996).Information privacy: Measuring individuals’ concerns about organizational practices. MIS Quarterly, 20(2), 167–196.
- McKnight, D., Cummings, L., &Chervany, N. (1998). Initial trust formation in new organizational relationships. Academy of Management Review, 23(3), 473–490
- Zhang, J., Reithel, B. and Li, H. (2009). Impact of perceived technical protection on security behaviours. Information Management & Computer Security, 17(4), 330-340.
- Eggert, A. (2006). Intangibility and perceived risk in online environment. Journal of Marketing Management, 22, 5-6, 553-570.
- Berner, A. (2003). “The post-modern consumer implications of changing customer expectations for organization development in service organizations” in A journal of Industrial psychology 29 (3),-1-10

Other reports

- Dhouha Jaziri, (2014), "From post modernism to postmodern consumer-The impact of consumer theory" in Lumen Research Centre in Social and Humanistic Sciences, Lumen Publishing House, ISSN 2068-0236
- Jain Mardav, (2019). The Aadhar Card: Cyber Security Issues With India's Biometric Experiment published by The Henry Jackson School of International Studies, 2019, 9th May
- Krishnan, S. (2018, July 13). How can Indian organisations prepare for the GDPR regime? Retrieved May 1, 2020, from https://www.pwc.in/consulting/cyber-security/blogs/how-can-indian-organisations-prepare-for-the-gdpr-regime.html
- Bhatia, G. (2018). The case against surveillance. Retrieved July 13, 2020, from https://www.thehindu.com/opinion/lead/the-case-against-surveillance/article25822069.ece
- Ministry of Electronics and Information Technology (MeitY). (2018). DATA PROTECTION IN INDIA [Brochure]. New Delhi, Delhi: Author. Retrieved from https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf
- Bureau, E. (2018). Justice Srikrishna committee submits report on data protection. Retrieved June 1, 2020, from https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-committee-submits-report-on-data-protection-herere-the-highlights/articleshow/65164663.cms?from=mdr
- The Personal Data Protection Bill, 2019. (2020, March 24). Retrieved June 1, 2020, from https://www.prsindia.org/billtrack/personal-data-protection-bill-2019
- Universal Declaration of Human Rights. (n.d.). Retrieved June 1, 2020, from https://www.un.org/en/universal-declaration-human-rights/
- IT Act 2000, Gazette of India Part 2
- The Indian Penal Code 1860, ACT No. 45, 1860
- Indian Copyright Act 1957
- Indian Contract Act 1872, ACT No. 9, 1872