e-ISSN 2582-4570

EMPIRICALLY UNVEILING THE POLICY & IMPLEMENTATION OF PRIVACY AND DATA PROTECTION LAWS IN DIGITAL INDIA

Dr.Jayanta Ghosh Dr.Ashwini Siwal***

Abstract

The up-gradation of the traditional system to the digitized system has made the life of the individual easy—this change is leading an individual to a vulnerable situation where his privacy is at stake. Organizations use individuals' data for earning billions of dollars. Multinational companies are using the user's patterns, public posts, and personal information of individuals for business purpose. Organizations are influencing the individual in such a way that they are made to think that in future, there will be no term like privacy, and the entire world is an open community. Liberty of an individual is being intruded by technological interference. Personal data protection laws are the subject matter of intense global debate, triggered by the extraordinary development of Information Technology (IT). This debate is primarily triggered by way of advancement in the technological sector interfering in terms of societal demand for regulation. The use of the Internet in the modern-day lifestyle has become indispensable, and the use of the Internet is making life easier. However, it has become a natural source to collect personal information and easily hack the servers storing the user data. Many internet users are not adequately educated on do's and don'ts of the Internet, and they became the victim. As a developing country, India doesn't have specific laws on privacy and data protection. There are several judicial pronouncements by the Apex Court that recognized the right to privacy. This research would foray to suggest the policy & implementation on privacy and data protection laws in digital India.

I. INTRODUCTION

Liberty is an expression that is valued in a dignified human life.[1] It is a natural law idea and a desire for human civilization.[2] Views are divergent as to what is essential for human life. A moral human being is one who at his capacity can think, reason, choose, and value things.[3]

*Research Fellow, Centre for Regulatory Studies, Governance and Public Policy, West Bengal National University of Juridical Sciences, India.
**Assistant Professor in IP & IT Laws, Faculty of Law, University of Delhi, India

[1]Weiss, Charles. "The Coming Technology of Knowledge Discovery: A Final Blow to Privacy Protection." *University of Illinois Journal of Law, Technology & Policy,* 253 (2004).
[2]Rawls, John. *A theory of justice*. (Harvard university press, 2009).
[3]Fried, Charles. *Modern liberty: And the limits of government*. (WW Norton & Company, 2007).

Liberty, which covers a variety of rights, raised to the status of distinct fundamental rights and other related rights.[4]

In order to endorse liberty, it is essential to preserve and protect the privacy of an individual; hence, privacy has to be treated as a right.[5] To understand privacy as a right, it is necessary to look to its origins and growth. It is also established that in history, there lies a relation of privacy and development of technology signifying the prominence of technology over privacy. In modern days, privacyhas become more prone in computerized information society.[6] From the times immemorial surveillance has set its roots. The Fifth Amendment of the Constitution of America has given the emphasis on privacy as an unreasonable search and seizure. International instruments like Magna Carta, Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), Convention on the Rights of the Child (CRC), International Convention on the Protection of All Migrant Workers and Members of Their Families, The European Convention on Human Rights and the American Convention on Human Rights all these acknowledge privacy rights.[7] To greater importance, privacy as a right has been recognized in the Universal Declaration of Human Rights (UDHR). To preserve the dignity of the human being as human rights, the UDHR has played an important role. It has inspired the constitutionalizing of privacy in many countries after the fall of imperialism. Article 12 of the UDHR focuses on the importance of privacy. It conveys that a person shall not be arbitrarily interfered with his privacy at family, home, or correspondence and not to attack upon his honour and reputation. Therefore, it can be said that that privacy requires non-encroachment of body and property by others without authorization.[8] The contents of the right to privacy have widened in the multi-dimensional sphere over a period of time viz, bodily privacy, territorial privacy, communication privacy, and information privacy (Privacy and Human Rights Survey). Amongst these mentioned privacies, communication privacy and informational privacy are two essential types of privacies that are directly related to personal information or personal data.

The sharing of personal data is subject to the will of a person. As regards human rights, there is no objection to the sharing of data or the exchange of data. In fact, it is often positively

[4]Bhattacharjee, Anandamoy M. *Equality, Liberty & Property Under the Constitution of India*. (Eastern Law House, 1997).
[5]Ibid.
[6]Viswanathan, Aparna. *Cyber Law: Indian & International Perspectives on Key Topics Including Data Security, E-commerce, Cloud Computing and Cyber Crimes*. (LexisNexis ButterworthsWadhwa, 2012).
[7]Baker, Tyler. Roe and Paris: does privacy have a principle. 26, *Stanford Law Review,* 1161 (1973).
[8]Benn, S. I. *Respect for Persons in JR Pennock& JW Chapman*, eds., (NOMOS XIII, Privacy, 1971).

crucial for the sharing of personal data to fulfil the obligation of the State to take steps to safeguard such human rights such as rights to life, and it can, in theory, be justified by reasonable considerations of public interest.[9] The exchange of personal information, however, eventually poses questions regarding human rights. In view of the welfare state claim, the policy must show that all data collection plans are both fair and proportionate and that sufficient protections are in place to ensure that personal data are not arbitrarily released unless it is rational in the circumstances.

The reason being, in this contemporary society, various activities of human beings are taking place in the virtual world and technology have become an integral part of human life. However, the goodness of technology has also brought along ill effects by endangering informational privacy in this technology-driven world where individuals, communicate, transact, and interact with others using advanced technology.[10] Here sharing of information is essential, as it is done voluntarily. Therefore, an individual should agree to face the consequences of disclosure of information. In this context, a State requires to consider that its institutional framework must focus on both aspects, i.e. privacy and data protection of an individual, (whether data is shared voluntarily or involuntarily).

II. STATEMENT OF PROBLEM

India has witnessed a rapid expansion of the use of the Internet amongst the inhabitants. At the same time, the digital divide which refers to the gap between demographics and regions that have access to information and communications technology, and those that don't or have restricted access, is also a reality in India. Information communication technology has been viewed as a solution to many ills, particularly, 'governance', as indicated in the broad vision of Digital India. The role of technology in improving governance, such as to bring transparency, more convenient access to services, etc., has been in place since the late 80s in India. Technology is used for distribution of different services/amenities by the government to the beneficiaries. This technology connects the citizen and government virtually.[11]

Virtual technology has made a distinct reflection on the human lifestyle. However, the lifestyle has also been made susceptible to individual privacy and data protection. The

[9]Bygrave, Lee A. *Data privacy law: an international perspective*, 63 (Oxford: Oxford University Press, 2014).
[10]Bygrave, Lee A. Data protection pursuant to the right to privacy in human rights treaties.6, no. 3 *International Journal of Law and Information Technology* 247-284,(1998).
[11]Bostwick, Gary L. "A taxonomy of privacy: Repose, sanctuary, and intimate decision. 64 *California LawReview* 1447,(1976).

concern of privacy and data protection becomes more pertinent because of the demographic pattern of the country where more than seventy per cent of the population lives in rural areas having inadequate/limitation of knowledge about technological interventions for claiming entitlements from the government. As the technological intervention is made compulsory for the program, sharing of information and storage of the same is *fait accompli* for individuals.

The government of India proposes Governance and Services on Demand to connect the beneficiaries with the government through the virtual world. It involves "using the Internet as a means to deliver services and information… [Which] allows users to register for government services".[12] Dempsey points out that *"privacy cannot be an afterthought in the design of information systems"* and for that matter, needs e-government implementation. Fairweather and Rogerson advise, *"e-government should also offer a good level of data protection and security".*[13]Therefore, the 'Digital India Programme' must also give preference to the privacy of an individual. Anderson points out that *"countries seeking to promote e-government must protect the privacy of the information they collect"*.[14] This imposes the responsibility upon the State to protect the collected information of the individuals. And the efforts of the government to protect individual privacy and data is in question.

III. BACKGROUND

The protection of information has been a serious concern; in this regard, international organizations has been pioneer. Protection of privacy and respect for human rights is a part of the fundamentals provided under the UDHR. As the UDHR is an outcome of the United Nations Organization (UNO), the responsibility lies in all the member states of the UNO to ensure the implementation of the UDHR and observe that all citizens are enjoying their human rights, without distinction. Amongst the list of human rights, *'personal liberty'* is one of the oldest human rights which was found in the Magna Carta as '*Libertatum'* of 1215. In this regard, the UDHR reflects that privacy is an integral part of personal liberty and in no means a separate institution. Article 17(1) of the International Covenant on Civil and Political Rights (ICCPR), Article 16(1) & Article 42(2) (vii) of the Convention on the Rights of the Child (CRC), and the Article 14 of International Convention on the Protection of All Migrant

[12]Chaffey, D., & Ellis-Chadwick, F. *Digital marketing*. (Pearson uk.2019).
[13]Fairweather, N. B., &Rogerson, S. Towards morally defensible e-government interactions with citizens. *Journal of Information, Communication and Ethics in Society*,(2006).
[14]Agyei-Bekoe, E., Empirical Investigation of the Role of Privacy and Data Protection in the Implementation of Electronic Government in Ghana,(2013).

Workers and Members of Their Families. At the regional level, the European Convention on Human Rights (Article 8(1)) protects the right to privacy and the American Convention on Human Rights (Article 11) provides legitimacy of the right to privacy.

In India, under Article 21 'personal liberty' is mentioned as a compendious term to include all the diversity of human rights other than those covered by Article 19(1).[15] While Article 19(1) covers specific species or rights attributes, personal liberty in Article 21 takes the residue in and consists of it. Expanding the contours of rights to 'Personal Liberty' and liberty, the apex court has held that privacy is an essential ingredient of liberty and freedom; hence, it enjoys the status of a fundamental right.[16] Informational privacy relates to the protection of data of an individual. Data or Information of specialized knowledge, facts, concepts including computer printouts magnetic or optical storage media, punched cards, punched tapes, etc. all of these comes under matters of informational privacy of an individual. The Constitution of India provides for the granting by the Supreme Court and High Courts of all rights therein to enforce fundamental rights or for other purposes, under Articles 32, 226, and 227. However, the availability of the writ for the enforcement of unenumerated rights or the right that falls short of clear enunciation through a judicial pronouncement is questionable. Now, there is a need to identify the position of the right to privacy on the landscape of enforceable rights and remedial measures available against the State in cases of violation.

In relation to privacy and data protection, the Information Technology (Amendment) Act 2008, have delineated some provisions. The preamble of the Act facilitates e-commerce *"which involves the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filings of documents with the Government agencies…"* Chapter III of the Act describes the electronics governance that dealt with legal recognition, retention of an electronic record, and digital signature, which has its limited applicability to procedural aspects. It also gives the power to make rules by the Central Government in respect of digital signature. The Act has limited applicability and fails to provide any legal mechanism about the sharing of information by an individual to the government for availing services or benefits under different schemes of *'Digital India*

[15]Singh, J. S. Expanding Horizons of Human Right to Education: Perspective on Indian and International Vision. *Journal of the Indian Law Institute*, *52*(1), 34-59.(2010).
[16]Rai, S. *Legal and Regulatory Issues of Privacy and Data Protection in e-Commerce: An Analytical Study* (Doctoral dissertation),(2020).

Programme' which is based on the horizontal relationship between the subject of the right holder and the duty-holder.

Considering that technological development, privacy and data protection are having a more significant impact on this digital age. The present-day scenario demands privacy and data protection to be read as a human right perspective. In this advancement of technological information era, the right to life and dignity of an individual requires a new dimension i.e. the least-intrusive role of the State. By the launch of the Digital India initiative, the government is preparing to make India a truly digital country by providing various e-government services across the different sectors through the cloud, connectivity, the Internet of Things, etc. With the implementation of the Digital India program, the privacy and data protection of an individual becomes a prominent concern.

IV. LEGAL SYSTEM OF INDIA AND DIGITAL INDIA

In accordance with Article 19(1) and Article 21, the Constitution of India is the bulwark of "democracy" and "liberty," which guarantees 'the right to freedom' and "personal rights.' Article 21's right to life was interpreted freely, in order to mean something more than mere survival, mere existence, or animal life. It includes, therefore, all those aspects of life which make the life of one man more meaningful, complete, and worthwhile. Privacy rights are 'the right to be alone.' A citizen has the right, among other things, to preserve his or her privacy, family, marriage, procreation, maternity, care for children, and education. The Supreme Court has held that the right to privacy is essential to the preservation of freedom.[17] Even though privacy and data protection have not been explicitly mentioned in any provision, 'privacy' as a right has evolved through various judicial pronouncements. In Article 21, personal liberty covers a variety of reasons and certain rights have fundamental rights and, in accordance with Article 19, additional protection. The right to expression limits the ambit of the private sphere of individuals, and therefore, there is a question of balancing two competing powers, i.e., speech and privacy. This right to privacy encompasses the protection of individual data or information; hence, arguably, both privacy and data protection are recognized as human rights.[18]

[17] *Gobind* v. *State of Madhya Pradesh and Anr*. (1975) 2 SCC 148.
[18] Sharma, S. *Data privacy and GDPR handbook*. (John Wiley & Sons.2019).

Considering the aspects as mentioned above, the recently announced initiative of the Government of India, the *'Digital India Programme'* needs to be examined against the touchstone of the legal regime on privacy and data protection. This program has been initiated as a policy of the government as of institutional arrangement for promises of better governance, inclusive growth, job opportunities, and quality of life to the citizen of this country through the intervention of Information Communication Technology (ICT). Three broad visions have been encapsulated under this program. One of the visions is 'Governance and Services on Demand' which targets seamless integration across departments or jurisdictions, services available in real-time from online and mobile platform, all citizens'entitlementsare to be made available on the cloud, services digitally transformed for improving ease of doing business, making financial transactions electronic and cashless, leveraging Geographical Information Services (GIS) for decision support systems. The targets envisaged under the vision will have a revolutionary impact on the governance of the country. The success of the program depends upon participation from an individual, particularly from marginalized and downtrodden sections of society for whom governance matters the most. To avail the benefits targeted in the program, every intended beneficiary needs to submit personal information with the agencies/authorities designated thereof. For full-fledged participation and involvement, individuals who are parting with the information need to be assured about the protection of data and effective remedial mechanism in case of infringement of his right.

The absence of clarity on the right to privacy and data protection on the landscape of human rightsraises serious apprehension about the exercise of power by the government in relation to the collection and usage of data. Therefore, it is pertinent to examine the position of privacy and data protection in the gamut of the right to personal liberty and the right to freedom guaranteed under the Constitution of India. In this regard, the study will be undertaken with the reference of the Digital India program of the Government of India as it is based on the collection of personal information and the concern of the informant about the security and safety of the collected information.

V. OBJECTIVES

With the justification of the problem statement, few objectives are framed, these are:

a. To identify and examine the position of privacy and data protection as a human right from the Indian perspective.

b. To analyze the importance/impact of privacy and data protection in the accomplishment of the Digital India Programme (DIP).

c. To suggest a suitable policy & implementation framework for the protection of privacy and personal data.

VI. METHODOLOGY

In order to attain the research objectives, the researchers have adopted both doctrinal and non-doctrinal methodology. For the purpose of the doctrinal study, an inquiry into the constitutional provisions, legal rules, principles, and doctrines governing the privacy issues are undertaken to ascertain their relationships with informational privacy, i.e., data protection as a human right. The analytical method is employed to critically assess the statutory provisions, judicial pronouncements, policies, and doctrines relating to privacy and data protection laws. It has helped the researcher to identify the gaps and to structure a new legal paradigm on the subject matter. The researcher has also traced the evolutionary process that led to the origin of privacy and data protection laws. The researcher has found that this is helpful to discover crucial clues as to why the protection of personal information of individuals needs to be addressed as a paramount legal concern in this technologically advanced age and also to understand the need for the right-based exposition.

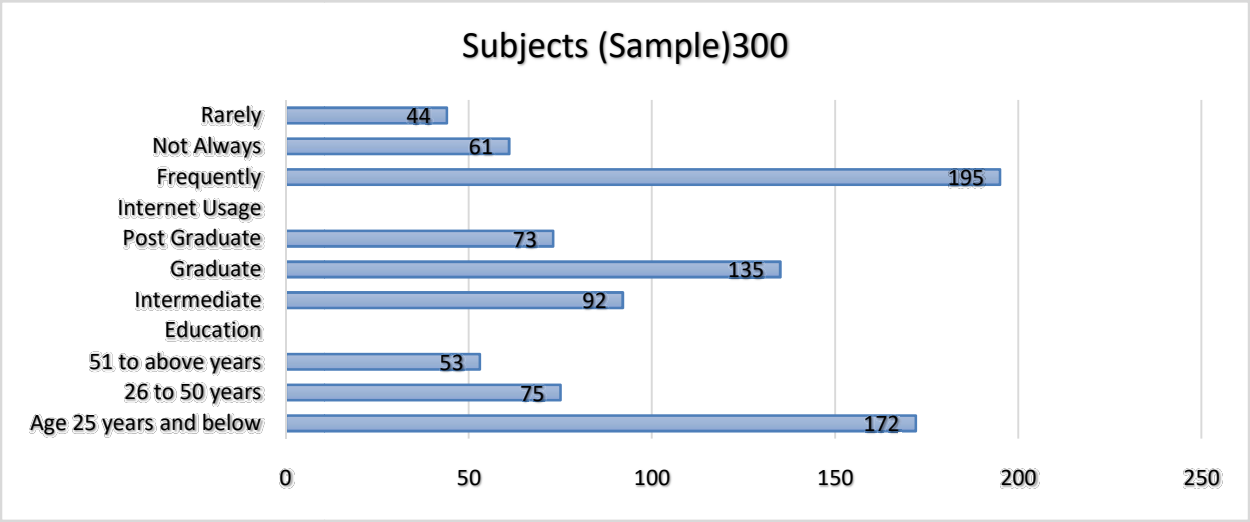
The researchers have conducted an empirical study, which ensured the validity and the authenticity of the emerging issues of privacy and data protection laws on the Digital India Programme. A structured questionnaire was framed according to the research objectives. The qualitative analysis is performed on the questionnaire-based survey. This survey is done with different stakeholders. Interview methods are used for data collection. These methods are chosen because of the direct access, one-to-one interaction with the stakeholders. It has facilitated an in-depth understanding of the Digital India Programme implementation process and privacy and data protection issues within it.

VII. SAMPLE

The samples do not show statistically representative of any particular community or technology users. Chart 1 summarizes the demographic information of the subjects. Subjects were statistically similar with respect to the usage of the Internet. Subjects were mostly general public, college-educated, and experienced Internet users. Therefore, it need not rule out the possibility that some of the differences observed among the subjects may be attributed to differences in gender, age, internet user, or education.

There are three broad groups categorized based on age, education, and internet usage. Further, each category is divided into groups based on different factors. In the age category, the samples are divided into three groups based on age. In the education category, the samples are divided into three groups based on educational qualifications. Lastly, in the internet usage category, the samples are divided into three groups based on the regularity of use of the Internet.

Chart 1.



VIII. INTERVIEW

The interviews conducted through one-on-one open-ended questions to gain insights into people's views regarding privacy and data protection. The interviews were conducted within India. The subject's sample was distinguished by their age, education, gender, internet user. Selected subjects were segregated into three categories with their age difference who were between below 25 years, 26 to 50, and above 50 years old. The interview made a total of 300 subjects, recorded their interviews, and produced in the form of text transcripts. This interview focused on the rights perspective of privacy and data protection.

This interview questionnaire was designed to analyze the right approach to privacy, data protection, and digital India. And, also on awareness and concerns about privacy for individual personal information, especially related to privacy, data protection, and digital India. Open-ended questions covered the following attributes:

1. General understanding and concerns about privacy and data protection.
2. Sharing personal information- consent aspect
3. Relief level of public sharing of information – different types of data
4. Awareness of Laws and Policies and the need for privacy and data protection laws.
5. Trust on government or agency authorized to collect information
6. Concerns about identity sharing with the government by Digital India Programme.

IX. SURVEY RESULT AND ANALYSIS

The empirical analysis is being done on the privacy and data protection and Digital India program. This research analysis helped to provide policy suggestions for India. In order to have accurate empirical analysis, the sample set is carefully collected by taking people from all sections of life and profession. The sample responses are collected and analyzed impartially. Conducting empirical analysis of the collected sample responses, this analysis shows the emphasis given by individuals to protect their privacy and personal data. The importance of privacy /data protection and digitization of India are interlinked among the six-notions set by the researcher to conduct a precise vibrant study. All six notions have their significance to identify the very basis of the conclusiveness of the study.

The interviews with samples/subjects are done in India. Interview methodology is loosely based on the mental model methods that are used in creating value communications. Likert scale is followed for the preparation of the questionnaire.

IX.I DIFFERENT ATTRIBUTE ANALYSIS

The analysis of the right based approach is carried out in six different segments in this. These are discussed as follows:

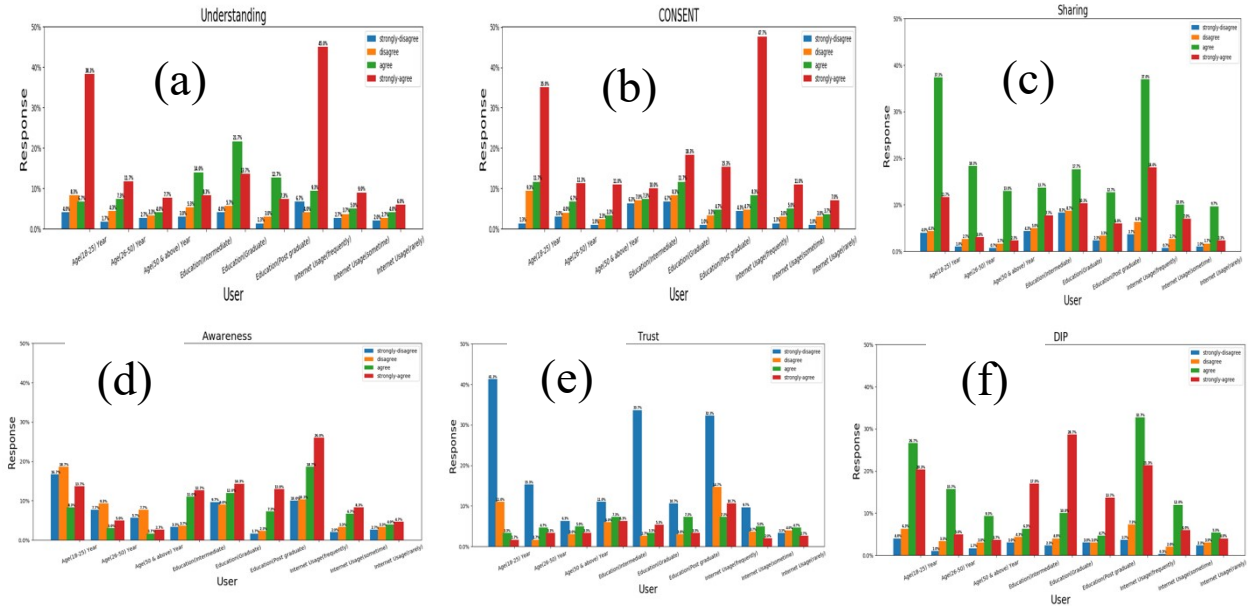


Fig.1

General Understanding and Concerns about Privacy and Data Protection {Fig 1(a)}.

The general understanding and concern about the privacy and data protection of an individual are inclined towards the security of information. So, with the responses of the sample according to the questionnaire, which is shown below in Graph (understanding), the samples across all the age groups have strongly agreed to protect privacy and data protection. In the age group, the first category (age 18 to 25 years) are more acquainted with the understanding of privacy as per the response collected. The reason behind that this category is equipped with the knowledge of technology and the loopholes therein. The samples across all the education categories have agreed to the protection of privacy and personal data. The graduate and post-graduate groups understand the nuances of privacy due to educational qualifications.Samples across all the internet user's categories have also strongly consented for the same. The percentage of the analysis is more aligned to strongly agree that they are concerned for the privacy and data protection.

Sharing Personal Information- Consent Aspect {Fig. 1(b)}

Consent for data sharing of information for a specific purpose is highlighted in this analysis. Here, the respondents have been asked to give views on giving consent to share the data for a pre-defined target, and the collected data should not be used for other purposes. The analysis appears to be divergent based on the concern of the people belonging to a particular age group. Different categories have expressed their view to get consent for every data collection and use of their personal information. In the age group, the first category (age 18 to 25 years) is more concerned about this than the third category (age 50 and above years). Older people do not keep themselves abreast of the latest technology. Thus, they are least concerned about the sharing of information for other purposes. But in the second group, all the three categories have significantly endorsed that there should be consent before sharing the information for a different purpose. In the third group, frequent users of the Internet have stressed consent before using the data for other purposes. The third internet usage group had strongly expressed positive response for the consent aspects by the frequent users. At the same, all three groups have heartily agreed with the consent aspect. Hence, all categories have more or less strongly agreed that the user consent issues should be taken and considered before sharing their data.

Relief Level of Public Sharing of Information – Different Types of Data {Fig 1.(c)}

The comfort level of the samples for sharing information publicly depends on various factors. The factors may be the use of different modern technology and taking benefit out of that. Indeed, the benefit of interest is the primary concern for the individual for making public his/her personal information. Personal information may be the factor to grow his business, peer group popularity, and respect/dignity of the individual. With the analysis of these factors, it is found that all groups' categories are in agreeable disposition. For example, the first age group of 18 to 25 years wants to become more famous by sharing their achievements in public, but the third category of age 51 and above are not interested in doing the same. In the internet usage group, frequent internet users are ready to share their information to some extent to the public as they know the consequences. But in the same group, the sometime-users of the Internet are pretty reluctant about this sharing. This analysis brings in a point that the people will accept the public sharing of information. It will further get strengthened by a promising legal regime which aims at the protection of data. Such a statutory scheme will build the confidence of the people in the system and will facilitate the government to employ technology for better governance for quality of life.

Awareness of Laws and Policies and Need for Privacy and Data Protection Laws {Fig. 1(d)}.

In terms of awareness level of the laws and policies on privacy and data protection, the responses are different in every category. By analysis of age group, the first category (18 to 25 years' age) and second category (26 to 50 years' age) have some knowledge of the laws and policies. In terms of education level group, the responses are inclined towards strongly agree. The graduate category of the respondent is more accustomed to the laws and policies. It is endorsed that the samples of post-graduation degree are better acquainted with privacy laws and policies. The same is also reflected in the response of frequent internet users, they are familiar with the laws and policies. Even the samples who rarely use the Internet are concerned about their personal information and privacy. The analysis conveys the trust of people on the law and legal system and reiterates the requirement of a specific law on data protection.

Trust on Government or Agency Authorize to Collect Information {Fig.1(e)}

The word 'trust' can be termed as here confidence to share something; it is only applied for privacy and data protection. By referring to the responses of the age groups, the first category (18 to 25 years of age) respondents have expressed the trust in negation. The second category (26 to 50 years of age) respondent has a similar viewpoint, but some of the respondents have some faith in government in specific issues like national security. And the third category (51 years and above) responses are more or less the same in relation to trust. The reaction of the samples on the education category also communicates the least reliance on the government agency. The category of internet usage indicated strong reservations to accept the fact that the government could protect the information. The sample responses are systematically analyzed to depict the fact that samples are not ready to keep their complete trust in government. This analysis is a telling one. It communicates that the enactment of law may change the perception of the people.

Concerns about Identity Sharing with Government by Digital India Programme {Fig. 1(f)}.

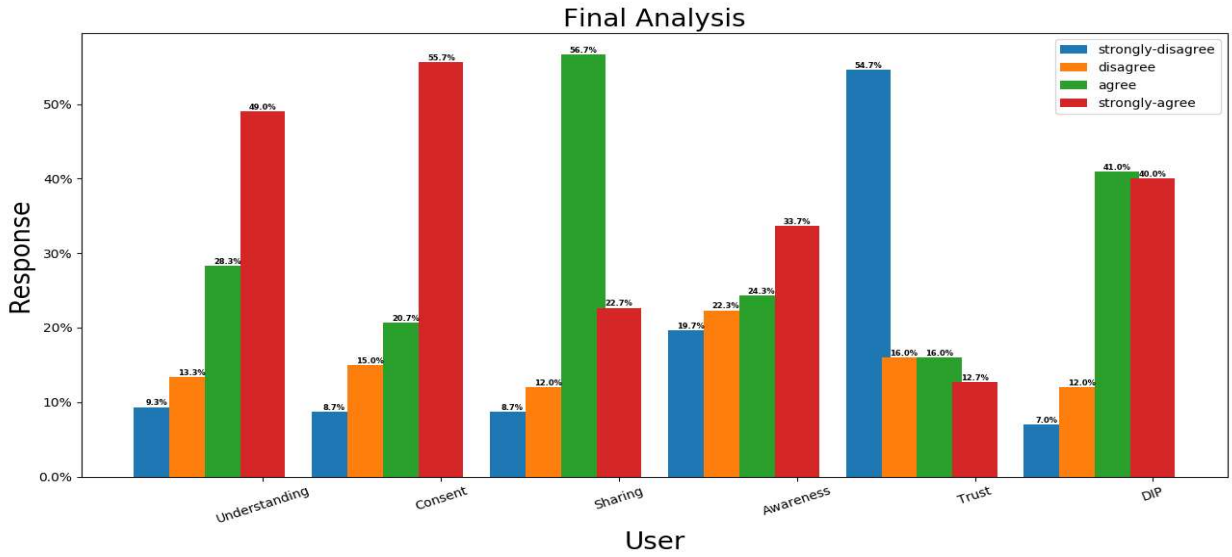
Ambiguity related to the protection of privacy and information in the Digital India Programme has created more confusion than clarity. Respondents of the sample survey also

spoke about this fact. Indeed, the concerns arose with the sharing of personal information with the government for getting the benefit of different social schemes. Sample responses analyzed so far, the first age group (18 to 25 years of age) have expressed their interest to hold and share personal information. The second category (26 to 50 years of age groups) is agreed on the sharing of personal information to get the benefits. To get the benefit out of schemes, individuals are sharing the information with the governments. The samples have expressed apprehension about the treatment of collected information by the government after completion of the welfare scheme. Will they still be used by the government or to be shared with the third-party agency? In the education category, the samples have indicated disapproval in identity sharing with the government under Digital India Programme. Every educational institution has made it mandatory to share the Aadhaar information for necessary identity purposes. This Aadhaar is the fundamental parameter to recognize and identify a persons' eligibility to benefit from any scheme provided by the government. The internet users' category also showed their reservation to share personal information.

Final Analysis

With the analysis of the six factors/notions (above fig.1), it is found that people are more inclined towards the protection of personal data. The acceptability towards the right to privacy as a fundamental right will make the State liable and will make it obligated towards privacy and personal data. The people are increasingly becoming aware of informational privacy with the adoption of technology in day-to-day life. Around 50 % of the respondents have exhibited their understanding of this issue. On the sharing of personal information, it must not be available to other organizations without any regulation or restrictions. Out of the total 55.67, percent of the respondent are strongly agreed for the consent clause to be added in sharing agreement. With the comfort level of public sharing, 56.67 percent of responses have clearly shown that the information available in the public domain must be guided by the principle of fairness so that the purpose of collection and usage should match. Any sharing of the collected information needs to be conditional, based on the public good. The ratio of awareness of the knowledge of laws and regulation is relatively average by 19.67 percent, 22.33 percent, 24.33 percent, and 33.67 percent across all the categories. With that response, it can be figured out that the awareness level is required to increase as the technology demands. In relation to the trust of the government agencies or organizations, the sample response is varying from each other. There are few concerns reflected by the sample

responses like organizational, technical security measures, and privacy policy. For that, the 54.67 percent responses are strongly disagreed on the trust factor/notion. About the Digital India Programme of the government, the sample responses are relatively similar as per the percentage of responses, and the trust to share the information is marginally equal on both the category. One aspect is that those who are willing to take advantage of the scheme they have to share the information. And the other segment is that who are not taking the advantage they are not interested in sharing their information.



X. CRITICAL ANALYSIS OF DIGITAL INDIA PROGRAMME (DIP)

Digital India is an initiative to build digital infrastructure and provide Internet access and online services to every citizen along with digital literacy to empower them to utilize the digital services effectively and avail all the government benefits efficiently. But due to gaps in its structure and services its effectiveness and thus it's enormous potential are diluted and could bring adverse effects to the security of the entire digital data in India. As an essential means of storing key documents such as Voter ID Card, Pan Card, BPT Card, Driving License, educational certificates, etc. in the cloud was introduced by Digi-Locker, for instance. This service would be provided to the citizens who are Aadhaar cardholders. The government of India would maintain the central repository for this service. Hence, personal information should be in the custody of the state actor. A state player may legally or illegally utilize this information at any point of time as necessary.

XI. EFFECT OF PRIVACY AND DATA PROTECTION ON DIGITAL INDIA

There is some futuristic effect of privacy and data protection on Digital India, and these are as follows:

1. The massive database of personal information is stored in public domains with protective firewalls around it. This will enable faster access to the authenticated user but at the same give opportunity to the hacker to steal information.

2. Personal information of the individual is stored in the public domain, because of that, the market structure of the State can be presumed. The future analytic decision for the development, needs, and the possibility of the human being can be shaped positively or negatively.

3. The privacy of the human being may not be in the hands of the individual. In the future, the individual may not be able to create any barriers to protect his/her privacy.

4. In future, the human can be categorized into two categories, one who wants to protect his private life but will not be able to preserve and other who don't even care about their personal private life.

5. With the technological up-gradation, the different new schemes of Digital India may require the up-gradation or forming of a new policy framework as the older versions may not be able to protect the personal information.

6. The third-party implication to collect, process, and disclose of personal information has made human being vulnerable. Countless organizations maintain records about us. They store documents and photos with cloud service providers. Credit card companies keep detailed records of our purchases. Our location information is available to telecommunications companies. Our Web surfing activity is in the hands of ISPs. Merchants such as Flipkart, Amazon have records about our purchases of books and movies and other things. Surprisingly, human beings are not able to understand the importance of this data, if this information falls into the hands of a third party may cause adverse effects to the individual.

7. This is a significant concern in which even the developed economies struggle to prevent. India being vulnerable to cyber-attacks, how the government is going to avoid these kinds of attacks were the stakeholders and people's concern. The whole

measures against cyber-attacks lie in spreading awareness among the people on how to use the Internet and personal data. The government must prevent its sensitive data from cyber-terrorism by using to latest technologies.

XII. CONCLUSION AND SUGGESTION

Privacy is a culturally sophisticated problem in our society, continually developing with time. It continually evolves with the changing state practices and judicial trends. Indeed, the concept of privacy is conflict-ridden, and thus, it keeps on perplexing the minds of the scholars who try to define it with precision. It is a fact that the centuries of cultural turmoil have made Indians more privacy-conscious than other western societies and to a certain extent conservative. Thus, in India, the legislature has the responsibility to consider our societal structure before framing any privacy laws. Additionally, a comprehensive legal framework on privacy law will contribute to raising the confidence of the people for whom the government designs the welfare program.

In this context, needless to mention that the personal data or information is very sensitive and important. But unscrupulous public and private players of our society are always playing around with our personal information. The sharing of personal information of an individual makes him particularly vulnerable in the society because the privacy breach and openly sharing of information will likely to put him in a 'Zero Privacy Zone'. Similarly, state surveillance and search in the personal property of an individual is a breach of the civil rights of that individual, as his right to privacy cannot be trampled by arbitrary and unreasonable state action.

For the comprehensive goal of privacy protection, it is required to maintain the balance between the sharing and respecting the importance of data privacy, which in turn can be ensured by forming proper data usage regulations within the organizational set up (public or private). Also, the idea of concurrent sharing and protecting data can only be possible when the data protection laws are followed rigidly based on the accepted principles. Also, the government needs to tap the benefit of technology for better implementation of the welfare program due to the large and diversified population with asymmetrical economic growth.

So far, the Indian judiciary has interpreted Article 21 to include the right to privacy. The analysis of the judicial approach reveals that every Indian citizen has a right to make his own

decisions. Thus, it can be said that the autonomy and dignity of the individual are the salient features of the right to privacy. True, that the people can claim and exercise their rights in the court of law. But the remedy may still elude them if such claims demand judicial action beyond the permissible limit set by the Constitution. Judiciary must conform to the constitutional mandate in interpreting certain key principles of privacy law: as the principles of privacy always support or protect individual autonomy and dignity.

XIII. FUTURE PERSPECTIVE

Today, every organization is maintaining personal records in such a way that any individual can be distinctly recognized. Similarly, the sensitive information embedded in the judicial documents should be protected in such a way that an individual does not face adverse social consequences. It is suggested that the need for data protection cannot be varied according to the position of the institutions of the country. Because the core component of a right cannot be given differential interpretation. The same protection may be accorded to both private and public domains. Advancement of technology also poses significant challenges as new sources are constantly being identified, and fresh methods of data collection are being introduced. Because of this, the experts throughout the world are required to be on their toes to tackle delicate issues emanating from those processes of advancements.