

## DIGITAL DIVIDE VS DIGITAL INDIA ASPECTS OF PRIVACY AND DATA PROTECTION IN INDIA

Dr. Jayanta Ghosh

*Research Fellow, Centre for Regulatory Studies, Governance and Public Policy, The West Bengal National University of Juridical Sciences, Kolkata, Email: jayanta.crsgrp@nujs.edu*

---

### Abstract

*Privacy and data protection issues in the modern era are forced to be re-examined due to the recent advancement of technology and the dynamism of the legal world. Although privacy has since become a privileged issue for everyone, today's emphasis is on data protection within the 'Digital India Programme'. Personal data is under threat when an individual shares information with strangers. As a result of the exceptional rise of Information Technology (IT), the dramatic growth of its devices' capacity to store, process, and link data, the discussion around personal data protection has intensified significantly. Because of the way it offers its products, the debate has been exacerbated. This use of products in human life style became vulnerable in terms of sharing information with a stranger on this technologically advanced epoch without knowing facts. The pervasive role of technology in day-to-day affairs of the individual has been causing vulnerability. Personal information disclosed, intentionally or unintentionally, has been exploited for commercial interest and susceptible to misuse. The right to protect one's information is a derivative of the right to privacy. The scope and ambit of the right needs to be constructed to build a right-based framework for personal information/data protection. With this introduction of the policy of the government of India there is a need for a specific re-examination of the protection of the individual privacy and data protection. In addition, research will be needed to understand its impacts/importance.*

**Keywords:** *Privacy, Data Protection, Digital India, Information Technology.*

---

### Introduction

A moral human being is one who at his capacity can think, reason, choose, and value things. However, in this scenario of divergent views, freedom and rationality are two milestones in achieving an individual's liberty. Further, an individual's right to express his thought and protect his personal privatism from encroachment is essential to enjoy his liberty. Liberty, which covers a variety of rights, raised to the status of distinct fundamental rights and other related rights of

right to privacy. Charles Fried, "Privacy" Fried argues that privacy is necessary for the maintaining of intimate and interpersonal relationships, because it allows for discretion as to whom one shares information with.<sup>1</sup> Judith Jarvis Thomson, "The Right to Privacy" Thomson is skeptical of privacy and argues that there is nothing coherent or distinctive about privacy as a legal or conceptual notion: there is not one central characteristic of

---

<sup>1</sup> Charles Fried, *The Nature and Importance of Liberty*, HARVARD JOURNAL OF LAW & PUBLIC POLICY, Vol 29, pp.3-8, (2005).

privacy (coherence) nor is it distinctive from other rights: property as one example. Privacy, then, is derivative of other rights.

Privacy has to be recognised as a right if liberty is to be supported.<sup>2</sup> Photography, computers, and personal data are just some of the more modern issues that today's discussion began with. With respect to bodily privacy, territorial privacy, communication privacy, and information privacy, the scope of the right to privacy has widened over time.<sup>3</sup> Communication privacy and informational privacy are two types of personal information-related privacy that is crucial in today's society. Personal information is shared at the discretion of men. Sharing of data, which includes such activities as giving your medical records to another doctor or uploading your photos to the internet, has no apparent negative impact on human rights. The State's duty to take steps to protect certain human rights, such as the right to life, may sometimes require the collection of personal data, and in some cases, it is theoretically justified based on public interest considerations. For the argument for the welfare state, government must present data-sharing proposals that are both justifiable

and proportionate, and evidence is provided to show that safeguards are in place to prevent personal data from being arbitrarily disclosed unless necessary.

India's Constitution is a cornerstone of freedom and liberty, providing the guaranteed rights of liberty and freedom according to articles 19(1) and 21 respectively. The rights mentioned in Article 21 of the UN International Covenant on Civil and Political Rights have been interpreted as meaning something more than simply surviving and simply existing. Life is better because it includes all those facets that enhance the value, meaning, and purpose of a person's life. To have the right to privacy is one of those facets. Right to privacy is 'a right to be let alone'.<sup>4</sup> The Supreme Court has held that the right to privacy is essential to the preservation of freedom.<sup>5</sup> Even though, privacy and data protection have not been explicitly mentioned in any provision, 'privacy' as a right has evolved through various judicial pronouncements.<sup>6</sup>

Considering the above-mentioned aspects, the recently announced initiative of the

<sup>2</sup> A M BHATTACHERJEE, EQUALITY, LIBERTY AND PROPERTY UNDER THE CONSTITUTION OF INDIA, EASTERN LAW HOUSE, NEW DELHI, p.55, (1997).

<sup>3</sup> Available at, <http://gilc.org/privacy/survey/intro.html> (last Updated April 15, 2017).

<sup>4</sup> Messrs. Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, HARVARD LAW REVIEW (1890).

<sup>5</sup> Ram Jethmalani and Ors. v. Union of India (2011) 8 SCC 1

<sup>6</sup> Jayanta G & Uday S, 'Privacy and Data Protection Laws in India: A Right-Based Analysis' *Bharti Law Review*, Vol. V, Issue.2, (Oct-Dec 2016), pp. 54-72.

Government of India, 'Digital India Programme'<sup>7</sup> needs to be examined against the touchstone of legal regime on privacy and data protection. This programme has been initiated as a policy of the government promising better governance, inclusive growth, job opportunities and quality of life to citizen of this country through intervention of Information Communication Technology (ICT).<sup>8</sup> The absence of clarity on right to privacy and data protection on the landscape of human rights raises 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 right to personal liberty and right to freedom guaranteed under the Constitution of India. In this regard, the study will be undertaken with the reference of Digital India programme of the Government of India as it is based on collection of personal information and the concern of the informant about the security and safety of the collected information.

### Goals – Looking for

India has witnessed rapid expansion of use of internet amongst the inhabitants. At the same

<sup>7</sup> Digital India Programme, Available at: <http://www.digitalindia.gov.in/content/about-programme> (Last updated April 10, 2017).

<sup>8</sup> Ibid.

time, the digital divide which refers to the gap between demographics and regions that have access to information and communications technology, and those that do not (don't = colloquial= or have restricted access, is also a reality in India. Information communication technology has been viewed as a solution of 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, easier access to services etc., has been in place since late 80s in India. For the purpose of distribution of different services/amenities by the government arrangement, through technology. This technology connects the citizen and government virtually.

Dempsey points out that "privacy" cannot be an afterthought in the design of information systems" and for that matter needs e-government implementation.<sup>9</sup> Fairweather and Rogerson advises, "e-government should also offer a good level of data protection and security".<sup>10</sup> Therefore, the 'Digital India Programme' must also give preference to the

<sup>9</sup> Anderson, P. and Dempsey, J. *Privacy and e-government: privacy impact assessments and privacy commissioners—two mechanisms for protecting privacy to promote citizen trust online*. GLOBAL INTERNET POLICY INITIATIVE, p. 11, (2003).

<sup>10</sup> Fairweather, N.B. And Rogerson, S. *Towards morally defensible e-government interactions with citizens*. JOURNAL OF INFORMATION, COMMUNICATION AND ETHICS IN SOCIETY, 4 (4), pp. 173-180, (2006).

privacy of an individual. Anderson points out that “countries seeking to promote e-government must protect the privacy of the information they collect”.<sup>11</sup> This imposes the responsibility upon the state to protect the collected information of the individuals. And the efforts of the government to protect the individual privacy and data is in question.

The privacy right has come up with another dimension i.e. data protection. Data protection as a right like the right of access to data banks, the right to check their exactness, the right to bring them up to date and to correct them, the right to the secrecy of sensitive data, the right to authorize their dissemination: all these rights together today constitute the new right to privacy. In relation to privacy and data protection, the Information Technology (Amendment) Act 2008, have discussed some provisions.<sup>12</sup> The preamble of the Act facilitates e-commerce ‘which involve the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic filings of documents with

the Government agencies...’<sup>13</sup> The Act has limited applicability and fails to provide any legal mechanism regarding the sharing of information by an individual with the government for obtaining services or benefits under different schemes of the ‘Digital India Programme’ which is based on horizontal relationship between the subject of the right holder and the duty-holder.

Considering the technological development, privacy and data protection are having greater impact on this digital age. The present day’s scenario demands privacy and data protection to be read as a human right perspective. In this information technological era, the right to life and dignity of an individual has acquired a new dimension of least-intrusive role of the state. By the commencement of the Digital India programme, the government plans to make India a truly digital nation by offering a plethora of e-governance services schemes across sectors by using cloud, mobility, Internet of Things etc. With the implementation of the Digital India programme, the privacy and data protection of an individual becomes a prominent concern of the informant. In relation to privacy and data protection of an individual, the Digital India Programme has no legal mechanism to protect the shared information.

---

<sup>11</sup> Anderson, P. and Dempsey, J. *Privacy and e-government: privacy impact assessments and privacy commissioners—two mechanisms for protecting privacy to promote citizen trust online*. GLOBAL INTERNET POLICY INITIATIVE, p. 11, (2003).

<sup>12</sup> INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008, available at: [http://deity.gov.in/sites/upload\\_files/dit/files/downloads/itact2000/it\\_amendment\\_act2008.pdf](http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf) (Last updated April 20, 2017).

---

<sup>13</sup> Ibid.

## Research Focus

There are certain research analysis has to be done to accomplish the Digital India Programme with this technological advancement era, Firstly, to analyze the importance/Impact of privacy and data protection in accomplishment of Digital India Programme. And Secondly, to frame some suitable policy suggestion for protection of privacy and personal data in Digital India Programme. To fulfill these two research objectives some questions are to be sorted out which are very much relevant for this study and can be helpful to trace the concrete solution for the objectives. Firstly, what are the constitutional and legal provisions relating to privacy and data protection and whether they enjoy the status of right in the realm of human rights landscape? And whether the vision of Digital India addresses the concern of privacy and data protection for intended beneficiaries and what is its legal implications?

## Methodology Stepwise:

**Step 1:** For the purpose of this doctrinal study an inquiry into the legal rules, principles and doctrines governing the privacy-liberty issues to ascertain consistency, coherence, efficacy and stability in the area of privacy and data protection law.

**Step 2:** Historical method will be employed to trace the evolutionary process that led to the origin of data protection laws. This will help the researcher to explore and appreciate the circumstances that require suitable legal framework to deal with the issue. The researcher anticipates that this may also be helpful to trace crucial clues as to why the protection of personal information of individual need to address as a paramount legal concerns of this technological advancement age and also to understand need of the right-based exposition in Digital India Programme.

**Step 3:** The Analytical method will be employed to critically assess the statutory provisions, judicial pronouncements, policies and doctrines relating to privacy and data protection laws. This would help the researcher to structure a new legal paradigm for India. An analytical study will conduct for analysis of the judicial pronouncement. The researcher will anticipate by this analysis the judicial take on the privacy and data protection laws.

**Step 4:** The researcher will adopt an empirical study, which will anticipate the validity and the authenticity of the emerging issues of privacy and data protection laws in the concern of 'Digital India Programme'. A structured questionnaire will be frame

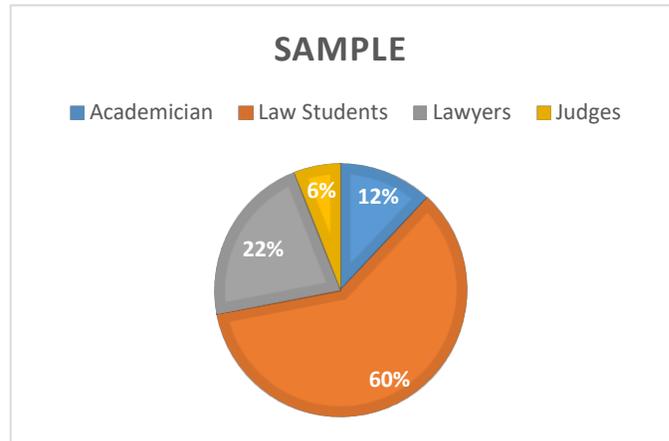
according to research objectives and questions. This qualitative analysis will be adopting on the questionnaire-based survey. This survey will be done with different stakeholders like, Academician, Law Students, Lawyers and Judges. Interview and focus group discussion methods will be used for collection of data. These methods will be chosen because of the direct access, one-to-one interaction with the stakeholders.

### Sample

Stakeholders	Sample
Academician	<b>60</b>
Law Students	<b>300</b>
Lawyers	<b>110</b>
Judges	<b>30</b>

These stakeholders are choose from different area of across India.<sup>14</sup>

<sup>14</sup> The sample includes graduate law students, professors from top Indian law universities, lawyers from different bar associations and Judges from different courts all over the country.



### Legal Journey Privacy to Data Protection in India

As a result of Article 21<sup>15</sup> of the Constitution and other constitutional provisions protecting fundamental rights, an individual's right to privacy has evolved. The Supreme Court of India has previously ruled in numerous cases<sup>16</sup> that the right to privacy is included in the fundamental rights of Indian citizens, such as the right to life and personal liberty. The only entity that may be held liable for constitutional violations is the state or state-owned entities, not private citizens or organizations.

The Constitution of India provides that *'No person shall be deprived of his life or personal liberty except according to the procedure*

<sup>15</sup> Article 21 of the Constitution provides that 'No person shall be deprived of life or personal liberty except according to the procedure established by law'.

<sup>16</sup> *Kharak Singh Vs. State of U.P* (AIR 1963 SC 1295; *Gobind Vs. State of M.P.* (AIR 1975 SC 1375; *R. Rajagopal Vs. State of Tamil Nadu* ([1994] 6 SCC 632); *People's Union of Civil Liberties (PUCL) Vs. Union of India* (AIR 1997 SC 568); *Distt. Registrar and Collector, Hyderabad Vs. Canara Bank* (AIR 2005 SC 186)

*established by law*' (Article 21). The Supreme Court has interpreted this provision to include the protection of privacy since *Kharak Singh v. The State of U.P.*, where it stated: '*It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty.*'<sup>17</sup> Personal privacy was also guaranteed by Articles 19(1)(a) and 19(1)(d), both of which mentioned freedom of speech and expression (right of freedom of movement).

Article 14 states "*equality before the law or the equal protection of the laws*"; both of these articles are important in relation to one another because of their mutual interaction. Article 19(1) (a) of the Constitution guarantees freedom of speech and expression to all citizens. In the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states, public order, decency, morality, contempt of court, defamation, and incitement of offence, the State may enact laws that restrict the exercise of the rights granted by Article 19(1). the Supreme Court has concluded that the right to know encompasses access to information contained in Article 19(1) (a).<sup>18</sup> All persons, whether or not they are citizens of India, have the right to equal protection under the law, as

<sup>17</sup> AIR1963 SC 1295

<sup>18</sup> State of U.P. v Raj Narayan (1975) AIR 1975 SC 865

guaranteed under Article 21. Authorities using the "procedure established by law" exception to Article 21 are instructed to strictly and meticulously adhere to all the legal requirements.<sup>19</sup> Since *Menka Gandhi v Union of India*<sup>20</sup> the phrase 'procedure established by law' has been held to have a meaning similar to 'due process of law' in the US Constitution. Case law has repeatedly taken a 'persons and not places' emphasis in interpreting the right of privacy, rejecting views that privacy is tied to property interests.<sup>21</sup> The ruling by the Indian Supreme Court is in line with the trend that started with the development of Article 21 in that it reflects a movement toward principles of data protection. However, this is only now happening: almost all Article 21 cases are about search and seizure or telecommunications surveillance. Outside search and surveillance issues, the most significant development has been the decision of the Delhi High Court in *Naz Foundation v. the Government of NCT of Delhi*.<sup>22</sup> The lawsuit was filed by the Naz Foundation, a non-profit organization, to challenge the constitutionality of Section 377 of the Indian

<sup>19</sup> Ram Narain v State of Bombay (1952) SCR 652.

<sup>20</sup> (1978) AIR 1978 SC 597

<sup>21</sup> District Registrar and Collector, Hyderabad & Anr. v Canara Bank & Ors. (2005) 1 SCC 496

<sup>22</sup> High Court of Delhi, Case number WP(c) No.7455/2001 (2 July 2009), available at <http://lobis.nic.in/dhc/APS/judgement/02-07-2009/APS02072009CW74552001.pdf>

Penal Code, which criminalizes “unnatural offences”, such as homosexuality, and others listed in the section's title. In 2004, the Supreme Court re-examined the matter, which the Delhi High Court had originally dismissed as an academic challenge.

The Court concluded that Section 377 (which bans gay sex) breaches the right to privacy, and it also denied the argument that there is an exception to Article 21 for laws that protect personal privacy. It was discovered that the state does not have the authority to invade citizens' privacy due solely to 'public morals'. Article 14 (equality before the law) and its more specific articulation in Article 15 were also found to violate (prohibiting discrimination on the grounds of sex).

The Naz Foundation Case seeks to go beyond issues of search and surveillance by advocating for the protection of personal privacy under the Indian Constitution. After conducting a thorough review of Indian case law on the issue of privacy, the Delhi High Court states that “A man's right to privacy can be found in the place where he can become and remain himself.” Individual autonomy enables each person to exercise the ability to do so. Whether this sweeping strategy could evolve in the direction of a "right to informational self-determination" developed by the German federal Constitutional Court

remains to be seen.<sup>23</sup> This is evident from the Supreme Court's work to define a right of access to public information prior to its national enactment in the Right to Information Act of 2005. The Supreme Court can make binding rules until the laws made by the legislature are found to be sufficient by the Court. It is necessary to bear in mind the possibility of future developments in the Indian judicial system when discussing the limits of Indian data protection law.

In the pronouncement of the Supreme Court expressed that *“Right to privacy is an integral part of right to life. This is a cherished constitutional value, and it is important that human beings be allowed domains of freedom that are free of public scrutiny unless they act in an unlawful manner.”*<sup>24</sup>

In *K.S. Puttaswamy v. Union of India*<sup>25</sup> the learned Attorney General asserted that *“the respondents do not share any personal information of an Aadhaar card holder through biometrics or otherwise with any other person or authority. This statement allays the apprehension for now, that there is a widespread breach of privacy of those to whom an Aadhaar card has been issued.”* This batch of matters involves important questions

<sup>23</sup> Judgment of 15 December 1983 (Census Act case), 65 BVerfGE 1

<sup>24</sup> Ram Jethmalani & Ors v. Union of India, Manu/SC/0711/2011, para 73.

<sup>25</sup> AIR2015SC3081

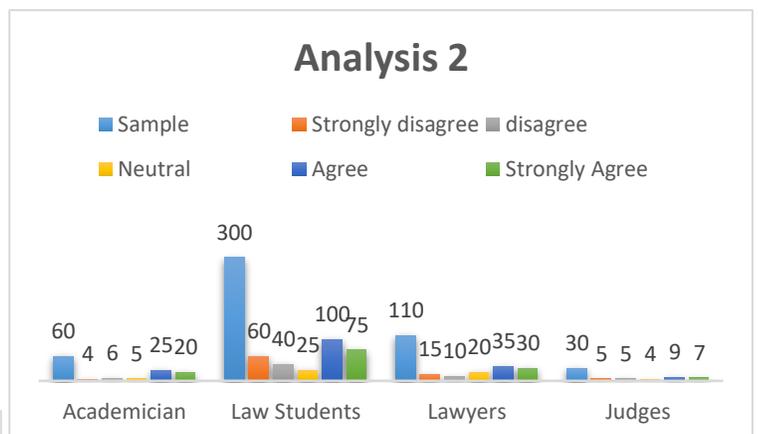
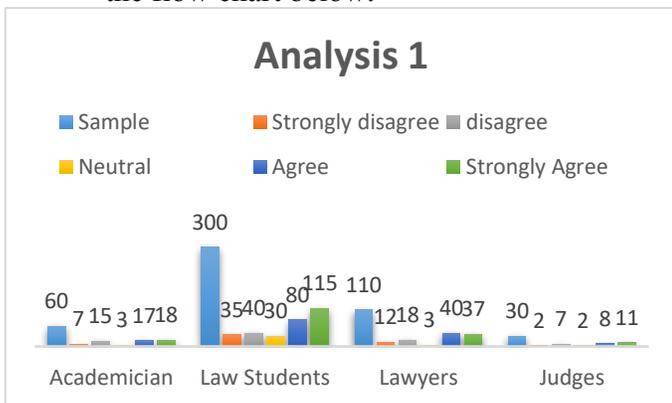
about whether a “right to privacy” is protected under our Constitution. Additionally, it must be recognised that if such a right exists, what are the sources and contours of the right to privacy, since there is no specific provision in the Constitution discussing the issue. As a result, these issues require a larger bench of at least five judges to hear and decide the matters based on the mandate in Article 145(3) of the Indian Constitution.<sup>26</sup>

**Results and Discussions**

**Analysis of the responses**

There are only four responses are taken for the completion of the empirical study. Total number of stakeholder sample 500 under four category namely, – academicians, law students, lawyers, judges. The sample responses analysis is shown in the flow chart below.

This response no 1, are taken in the context to get exact status of the privacy and data protection on digital India program recently launched by the government of India. Responses of the different category are more agreed on the position of privacy and data protection should be taken care separately. Strongly agree parameter given clear picture of the viability of the privacy and data protection. And also, the agree parameter is side by side supporting the position of the strongly agree.



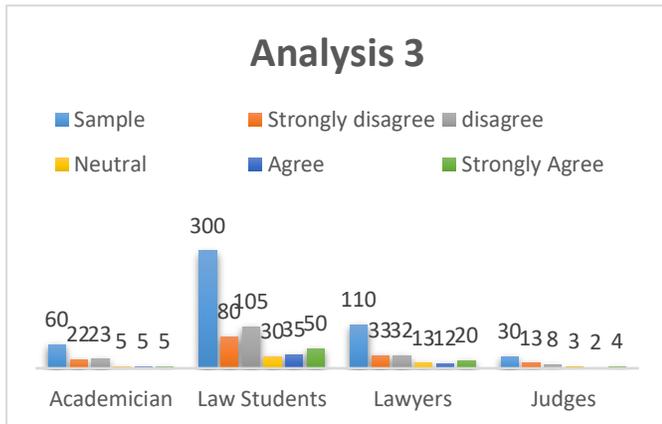
**Response 1:** Privacy and Data Protection are required separate status to deal with the Digital India Program.

**Response 2:** There is a need for separate regulatory body to maintaining the confidentiality of individual ‘Privacy’ & ‘Data Protection’.

In response no 2, for implementation of the separate regulatory body to maintain confidentiality of the individual privacy and data protection position is in agreeable position. This statements though not getting the up to mark for strongly agree parameter. In that, several situations come out like, who is

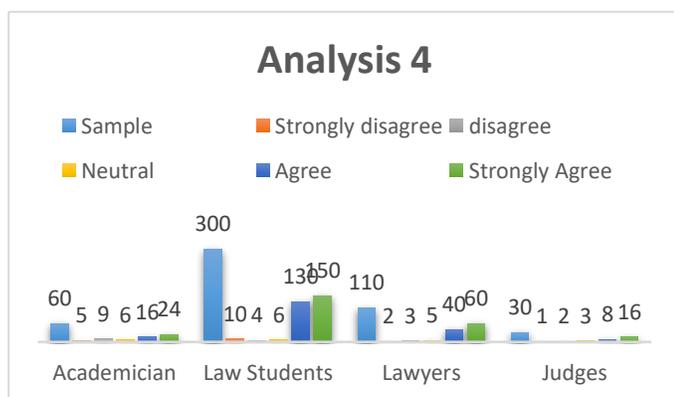
<sup>26</sup> Ibid.

the main regulatory body to process and stored the personal information, by whom this regulatory body would be selected, etc. So in terms of addressing this issue the result came out that the agree position is satisfactory.



**Response 3:** Existing laws are sufficient enough to deal with this Digital India Programme legal issues.

The response no 3, existing laws like Information Technology (amended) Act 2008, are sufficient enough to deal with this digital India programme, by this statement the ratio of responses are really astonishing that the stakeholders believe that it's not going to help for the individual privacy protection. Hence the statement strongly rejected by the stakeholders.



**Response 4:** 'Data Protection Laws' in India is required.

In the response no 4, for the legislation of the data protection laws the statistical parameter is more lenient on the side of the strongly agreeable portion. Hence the implementation of the data protection laws for the sake of the individual interest is given greater emphasis by the responses.

**Conclusion & Strategic Solution**

In this particular case study of privacy and data protection in digital India, the human right to data protection was definitely weighting more. Because someone's private information has the same value as someone's right to express his/her owns beliefs, when that person uses a third party's private information with no consent. The attempt is made in this monograph to answer the societies growing issue of digitalization of India and human tendencies to adaption of this. The basic idea is demonstrated with the analysis of these four responses of the different stakeholders of the Indian society for the viability and need of privacy and data protection laws. As well as this monograph argues that self-management of the sharing of personal data to avail the scheme benefit should be viewed as complementary tools to facilitate effective control as a human right. Individual can have

their subjective control on the personal information, yet the control must be buttressed by an architectural design of technology which should be regulated by laws and these laws should be made by following the golden principles of data protection.

Data protection is a fundamental right, and these separate fundamental rights should be recognized and granted for this reason. Many people are unaware that their personal information is protected, which allows authorities, internet service providers, and online businesses to commit numerous abuses against them. One thing we can hope for is that in time, people will understand the importance of fundamental data protection rights. Personal information security awareness should be at every level of society, and ethics should be kept in place so that organizations cannot abuse the personal information they have on others.

## REFERENCES

[1] Anderson, P. and Dempsey, J. Privacy and e-government: privacy impact assessments and privacy commissioners—two mechanisms for protecting privacy to promote citizen trust online. Global Internet Policy Initiative, p.11, (2003).

[2] Andrew Murray, Information Technology Law- The law and Society, Second Edition, Oxford University (2010).

[3] Anjali Agarwal, *Data Protection and Privacy Laws*, The International Journal of Science & Technology (ISSN 2321 – 919X).

[4] Charles Fried, The Nature and Importance of Liberty, *Harvard Journal of Law & Public Policy*, Vol 29, (2005).

[5] Daniel J. Solove & Paul M. Schwartz, *Privacy, information and technology*, Wolter Kluwer Law & Business Publisher in New York, (2011).

[6] District Registrar and Collector v. Canara Bank, (2005)1 SCC 496

[7] Fairweather, N.B. and Rogerson, S. Towards morally defensible e-government interactions with citizens. *Journal of Information, Communication and Ethics in Society*, 4 (4), (2006).

[8] Gobind v. State of Madhya Pradesh and Anr. (1975) 2 SCC 148

[9] Graham Greenleaf and Sinta Dewi Rosadi, Indonesia's data protection Regulation 2012: A brief code with data breach notification, *Privacy Laws & Business International Report*, Issue 122, (2013).

[10] Graham Greenleaf, Global data privacy in a networked world, Chapter in Brown, I (Edition) *Research Handbook on Governance*

- of the Internet Cheltenham: Edward Elgar, (2012).
- [11] I.C. GolakNath and Ors. v. State of Punjab and Anr. AIR1967SC1643
- [12] Justice Ajit Prakash Shah, Group of Expert on Privacy, (2012).
- [13] Jyoti Siwach & Dr. Amit Kumar, Vision of Digital India: Dreams comes True, IOSR Journal of Economics and Finance (IOSR-JEF) e-ISSN: 2321-5933, p-ISSN: 2321-5925. Volume 6, Issue 4. Ver. I (Jul. - Aug. 2015), PP 66-71
- [14] Kartar Singh v. State of Punjab MANU/SC/1597/1994
- [15] Kharak Singh v. The State of U.P. and Ors. AIR1963SC1295
- [16] Lee A Bygrave, Data Privacy Law- an International perspective, Oxford University Press, (2014).
- [17] M P Jain, Indian Constitutional Law, 6<sup>th</sup> Edition, Vol 1, LexisNexis, Butterworth's Wadhwa, Nagpur, (2010).
- [18] M.P. Sharma v. Satish Chandra MANU/SC/0018/1954
- [19] Maneka Gandhi v. Union of India, AIR 1978 SC 597
- [20] Messrs. Samuel D. Warren and Louis D. Brandeis "*The Right to Privacy*," Harvard Law Review (1890).
- [21] Mustafa Faizan, Emerging Jurisprudence of Right to Privacy in the Age of internet, Collection & Transfer of Personal Data- A Comparative Study, Kashmir University Law review, Vol XI, No XI, (2004).
- [22] Natasha Vaz, "Privacy: RTI, UID and Surveillance", April 29, 2012 at <http://privacy-india.org/2012/04/29/privacy-rti-uid-and-surveillance/> (Accessed on 25 Feb 2015).
- [23] National Data Sharing and Accessibility Policy 2012.
- [24] Nicholas D. Wells, Poorvi Chothani and James M. Thurman, Information Services, Technology, and Data Protection, The International Lawyer, Vol. 44, No. 1, International Legal Developments Year in Review: 2009, (2010).
- [25] Paul Lambert, A user guide to data protection, Bloomsbury Professional, (2013).
- Pawan Duggal, Data protection Law in India, Universal Law Publishing Co. Pvt. Ltd. New Delhi, (2016).
- [26] Peoples Union for Civil Liberties (PUCL) v. Union of India, AIR 2003 SC 2363
- [27] R.K. Chaubey, "An Introduction to Cyber Crime & Cyber Law", Kamal Law House, Calcutta, (2009).
- [28] Ram Jethmalani and Ors. v. Union of India (2011) 8 SCC 1
- [29] Registrar and Collector, Hyderabad and Anr.v. Canara Bank Etc AIR 2004 SC 935;

[30] Report of the Second Press Commission, Vol 1, (1982).

[31] S.K. Sharma, “Privacy Law: A Comparative Study” Atlantic Publishers & Distributors, (1994).

[32] Susan Herman, L. Simonson, On Privacy: Constitutional Protection for Personal Liberty,

48 N.Y.U. L. Rev. 670 (1973).