ELECTRONIC GOVERNANCE: A DELICATE BALANCE BETWEEN DATA PRIVACY AND FUTURE DIGITIZATION

Dr. Vinay Sharma[*]

Abstract

The development of network technologies has led to the growth of digital information all over the world. India has witnessed a rapid proliferation of the use of information and communication technology in the delivery of government services. E-government is seen as an instrument to simultaneously increase the efficiency, transparency and accountability of public administration and improve public service delivery. These developments have implications and pose challenges for privacy and security. Growth in this area has led to a proliferation of tools that collect data while Governments everywhere are trying to usher in an era of E-Governance. The endeavour is to improve the delivery of public services and to simplify processes that are associated with multiple levels of Government. In an effort to take this idea of E-Governance forward the National E- Governance Plan seeks to bring public services closer to the citizens of India. Data which is being exchanged in E-Governance is basically an heterogenous interconnectivity between public sector and private sector in which the data exchanged is voluminous. Citizens in general have welcomed the idea of E-Governance but data interchange has increased manifold and has raised concerns about the privacy of their data and the risk of it being compromised by parties privy to it. The proper implementation of E-Governance requires decentralization at all levels within the Indian governing mechanism. This paper looks at the major issues faced during the transition to a total E-Governance model. It examines whether the implementation of these E-Governance projects do address the issues of Data Privacy and security in wake of the implementation of the Data Protection Bill envisaged by the Government as the big game changer in every sphere.

[*] Asst. Professor @ Mahindra University, Hyderabad

INTRODUCTION

In the present era, Governments have made it a primary responsibility to provide citizens at their doorstep, public services governance is brought to the citizens and there is an endeavor to transform the relationship between Governments, businesses and the citizens of the country by implementation of these practices and procedures. Information technology has been the major force to make the provision of services available to everyone in an efficient and transparent manner, which has saved cost and led to a better degree of efficiency.

Electronic Government (e-government) has been at the forefront of local and national Governments during the last decade. Electronic Governance has been the essence where information technology has been applied in order to create 'Simple, Moral, Accountable, Responsive and Transparent' (SMART) Governance. As Electronic Governance has expanded it has transformed relations with businesses, citizens and other areas where it has resulted in improved interaction between the industry and Government, delivery of government services to the citizens and has also empowered citizens by granting access to information of government departments which has led to efficient management by Governments. The resultant benefits are less corruption, increased transparency, greater convenience, revenue growth and cost reductions[1].

As Electronic Governance and information technology have taken rapid strides there is a need to focus on the interface between the Government, local authorities and citizens. The advances in information technology and the internet have provided opportunities to the people and business to become a part of the process of governance. As different States in India endear themselves to the introduction of comprehensive Electronic Governance there are a large number of projects which are being implemented in the public – private partnership mode. As individual services are brought closer to the citizens and businesses there is a need for Governments to provide public delivery service mechanism through technology but in key areas there are challenges both in the macro-economic environment and also at the micro-economic level.

Electronic Governance can result in saving of capital and revenue expenditure[2] to governments and citizens alike, enhance transparency[3] and mitigate corruption[4]. Technology has now made it

[1] The World Bank, IBRD & IDA, understanding poverty, digital development, e-Government, May 19, 2015.
[2] Tapscott, D. (1996), The Digital Economy, New York, McGraw Hill.
[3] Mukhopadhyaya, Ashok (2000), IT and Administrative Culture, Indian Journal of Public Administration, 56 (3), pp. 293 – 299.

possible to a point of delivery where the specific needs of an individual can be looked into through the provision of Electronic Governance especially in countries like India. As Electronic Governance tools have become important there are still challenges before Governments with regard to automation, modernization, etc., which still require attention. Ordinary citizens in India have found it difficult to access internet and a serious challenge in Electronic Governance and digitization has been the protection of personal information with others, providing consent from the citizens for access to personal data, protecting personal data along with archiving it and the right to be forgotten.

It has also been observed that as fundamental privacy principles are compromised in Electronic Governance there is a need for trust, security and to understand the perceived risk that emanates from the use of technology and the uncertainty that is associated with online based transactions, cyber-attacks which have led to hacking of Electronic Governance systems. The endeavor of this paper considering the corpus of literature and insights is to bring to the fore the concerns of data protection and date privacy in the Indian and global scenario so that proper systems may be put into place before The Personal Data Protection Bill, 2019 could be enacted by Parliament.

OBJECTIVES

- To study implications of data privacy on behaviour of Electronic Governance systems.
- To evaluate the perceived risk that is associated with the Electronic Governance system.
- To recommend the strategy based on critical analysis of prevailing Electronic Governance policies.

HYPOTHESES

H1: Perceived Data privacy is ineffective in the current Electronic Governance norms.

H0: Perceived Data Privacy is effective in the current Electronic Governance norms.

REVIEW OF LITERATURE

The digital divide that has been described so capably by others has been found to affect user willingness to use e-commerce web sites (Thomas and Streib, 2007).

[4] Wescott, Clay.G (2003), "E-Government Supporting Public Sector Reform and Poverty Reduction in the Asia Pacific Region", in Stephen Howes, Ashok.K.Lahiri and Nicholas Stern (eds), State Level Reform in India, towards effective Government, Delhi, Macmillian

The information system literature abounds with studies describing how the resistance of users to a new system because of trust or other factors invariably hinders its implementation (Adams et al, 2004, Aladwani, 2001)

While there seems to be substantial growth in the development of e-government initiatives (Bednarz, 2002; Friel, 2002), it is not clear that citizens will embrace the use of such services. Some key concerns can limit this growth, including privacy (Thibodeau, 2000).

The General Data Protection Regulation (GDPR), which the European Parliament and Council enacted in the year 2016, is considered to be one of the best made security and privacy law in the world. GDPR has always been firm on data privacy, security and when people are entrusted with personal data through cloud services and has special laws on data breach.

The right to privacy under GDPR has been a part of the European Convention on Human Rights, 1950 and each Member State can implement its own law but they do need to adhere to the European Data Protection Directive, 1995 so that minimum levels of security and privacy are maintained. It has given protection to persons on their rights, freedom on data processing, data integrity, protection from processing of data unlawfully; fairness, transparency and accountability are included as the important facets of GDPR.

Member states can also create or introduce specific requirements, for lawfulness of processing. Articles 4, 8 of GDPR have given special conditions for children's consent and the same is attributable to the data controller. Article 9 of GDPR looks at sensitive personal data and additional categories has been created in both.

Under Articles 14 to 18, Articles 20 to 22 and Article 7(3) important rights are given under GDPR like Data Portability, object, erasure, profiling of data etc., and additional security measures have been recommended under Article 30, 32, 33, 35, 37 for impact assessment and security of data processing. Compensation under GDPR is a right under Article 82 and Article 82(2). Redressal is a matter of right under Article 77, 78, 79 whereas data transfer covers international organizations as well under Articles 44 to 50.

In a gist, GDPR looks at protection of natural persons, fundamental rights and freedom and freedom of movement with special reference to personal data.

Consent of a data subject under GDPR is a strict set of rules in which Government organizations cannot use information if consent is withdrawn by the data subject, children who are aged below 13 years can give consent with parent permission etc.

The challenge of privacy has to do with privacy violations or infringements based on inference (Barocas and Nissenbaum, Cambridge Books Online).

The Personal Data Protection Bill, 2019 has recognized that privacy rights are fundamental rights and the same the basis can be observed under Article 21 of the Indian Constitution. Section 43A along with Section 87(2) (ob) are to be omitted to keep personal data secure and protected. It would not be applicable to the processing of anonymized data unless it is directed by Central Government by the provisions of Section 91 of the Act.

This Bill has provided for data fiduciaries notified by the Data Protection Authority of India along with social media intermediaries. Sensitive personal data has been categorized like data related to finance, health, genetic, sexual, biometric, transgender, along with many other aspects of caste, tribe etc. It has been seen that data protection obligations under the Bill has set out a list of them as the role of the Data fiduciary, collection and process of data which is personal and how this data can be passed on outside India subject to conditions. Another important part of privacy is the right to be forgotten in which data taken by the data principal in consent under Section 11 then subsequently such consent has been withdrawn which has given data privacy a big fillip.

Clause 16 has dealt with the personal data of children along with its processing of the personal data involved as a very important aspect of security. Clause 25(1) has made an important contribution on the data fiduciary who has processed personal data and the same is breached which has caused harm to the data principal and this form of breach should be reported to the authority with all relevant details. Under Clause 41(1) the Data Protection Authority of India shall be established is a corporate body which has perpetual succession and shall be a body corporate with perpetual succession, a common seal and powers to hold and dispose properties which are immovable and movable and by the name allotted under the provisions of the Companies Act, 2013 has a provision to sue or be sued. Different forms of penalties and compensation have been envisaged under Clause 58 to 63 for penalties and Clause 64 for compensation. Appellate Tribunals are an important part in the new Personal Data Protection Bill, 2019 an appeal can be made to this Tribunal under provisions of Clause 72 and this

Tribunal shall not be bound by the Code of Civil Procedure, 1908, be based on the guiding principles of natural justice and certain another proviso that are given under the said Act. The Bill contains certain ambiguities which need to be resolved and the Government has invited recommendations and suggestions to the aforesaid Bill and has also included major portions from the GDPR in the new Personal Data Protection Bill, 2019 now being presented to the Indian Parliament and it could be a path breaking law in the near future.

China's personal privacy law which has come in the form of Personal Information Protection Law (PIPL) has taken restrictions but the major idea is to rein in the growth of technology giants like Tiktok, Bytedance, etc. The major concern is that PIPL is based on European GDPR but the State is able to access every citizen's personal information including his personal life.

RESEARCH METHODOLOGY

The research methodology primarily comprises of employing particular processes and procedures through various techniques of observation, identification, selection and finally analysis and evaluation of relevant data and information vis-à-vis to the tile, objectives and issues of the given research questions and problems. While engaging the research work of this study, an appropriate blend of quantitative, qualitative, descriptive, applied and analytical and case study research methods has been employed.

Additionally, in order to accommodate the digital and Electronic Governance aspects and implications of the available research data, secondary data has been used as a necessary component of the analysis and evaluation of quantitative and qualitative implications of the online available research articles, policy papers, bills, supreme court cases vis-à-vis to exploration of concerns of data protection and data privacy, specifically in Indian context; and generally, in global context. So that a more precise observation study can be made and an informed resolution can be reached with the pre-determined research objectives.

A LOOK AT THE ELECTRONIC GOVERNANCE FRAME WORK – DIGITIZATION OR PRIVACY

Electronic Governance in India has been a steady process in India which started with the computerization of Government departments and there has been sincere endeavour by the Government to improve the platforms public services are delivered to the people along with simplification of processes to access such services. The National Electronic Governance Plan

(NeGP) has tried to build on a massive infrastructure so that large scale data can be reliably accessed through the use of the internet and the major objectives is to make available public services to every citizen, business, Government. The Government wants to promote Electronic Governance through NeGP and they have integrated health, education, public distribution systems to be an ongoing project for making every form of Government service accessible to the citizens of the country. The Government of India under the NeGP has twenty-seven projects which are in the mission mode and an extra eight modes was propounded in 2006 and the number of projects that are under this mission mode was increased to thirty-one and these projects under the mission mode are being implemented by the Ministries that are under the Central Governments, State Governments and departments that belong to the State so that it can be aligned with the objectives of NeGP. The growth of the NeGP Programme has led to new initiatives by the Ministry of Electronics and Information Technology to include:

- Social Media Framework & Guidelines for Government Organisations.
- Citizen Engagement Framework for Electronic Governance Projects
- Saaransh – A Compendium of Mission Mode Projected un NeGP.
- National Information Technology Policy.
- E-Pramaan and G-I Cloud, an initiative which will ensure benefits of cloud computing for Electronic Governance projects.

The envisioning of such projects can be attribute to the Ministry of Corporate Affairs (MCA) 21 Project by the Government of India which is integrated with the National Electronic Governance Services Gateway (NSDG) has changed the way companies interact with Government now. As MCA 21 has improved speed and certainty and provides a blend of control and facilitation. The MCA 21 has more than 5 crore pages of corporate paper documents and within a seven-month period they have implemented and migrated under NEGP Program to a virtual complete paperless system. The MCA 21 which is operated on the BOOT model which is build, own, operate and transfer has digitized major projects and made them accessible to consumers. NEGP has also moved into pensions, income tax, passport, immigration, visa and foreign registration and tracking (IVFRT), central excise, banking, national residents/citizens data base, unique identification project [UIDAI (Aadhaar)], E-Office MMP, Insurance, E-Courts, E-Trade, etc.

SCOPE AND FORM OF ELECTRONIC GOVERNANCE INTERACTIONS

	Government	Business	Citizens
Government	G2G/G2E	G2B	G2C
Business	G2B		
Citizens	C2G		

On the basis of interactions, it can be seen that the interaction between Government, business and the citizens can be broadly correlated into the areas as per the Electronic Governance structure that is propounded by the NEGP. In a Government to Government (G2G) the flow of information and services has been made easy as to increase the flow of information horizontally i.e., between agencies that belong to the Government along with various departments which has led to vertical flow of information between Governments at various levels. In Government to Citizens (G2C) the citizens want availability and accessibility to public services in which they demand efficient delivery of public services to their door step. This mode of Electronic Governance has improved the standards of services which are being offered by governments and has increased citizen's participation in governance to the greatest extent possible and the Government has been more responsive to public needs.

In a Government to Business (G2B) Electronic Governance tool the objective has been to provide licensing, revenue collection, permits etc., by reducing time, process and procedures and create a transparent business environment so as to facilitate change. These models of categorization of Electronic Governance can be considered to reach its ultimate goal by making the citizen a part of the governance process that he is not only a consumer but a part of e-government too.[5] As the Government has brought in rapid changes in the e-government system the implementation can be identified in a multi- stage as follows:

- In any Electronic Governance process, the Government has to disseminate information through websites and the biggest challenge is to ensure that the information which is available is timely and accurate.

[5] Mintron, M. (2003), "Market Organizations and Deliberative Democracy; Choice and Voice in Public Service Delivery", Administration and Society, Volume 35 No.1, pp. 52-81.
Thomas, J and Streib, G. (2003) "The New Face of Government; Citizen Initiated Contacts in the era of E-Government", Journal of Public Administration Research and Theory, Vol. 13, No.1, pp.82-102.

- Electronic Governance requires communication between the stake holders and the information should be carefully deciphered and must be communicated to without loss of privacy.
- Government services must be integrated through a single window and the biggest challenge in Electronic Governance has been the integration of back office processes which consumes time and also a huge budget.
- Electronic Governance works under a decision making and planning process in which Law and policy are constraints which limit the Government powers and to complete the e-government projects.
- E-government is process which requires initiatives, appropriate capital expenditure investments into the core infrastructure of hardware and software, firewalls, spyware, malware etc., since data is stored.
- The maintenance of data by the government is dependent on trust as an important factor to determine the citizens/business willingness to use these Electronic Governance tools.
- Security in the context of e-government and data security policies, cyber security measures and stringent administrative and technical procedures are essential for citizen's trust in Electronic Governance.

As Electronic Governance in a large country like India has waded through various challenges the major concerns regarding infrastructure, technical constraints along with privacy and security are still being debated by the Ministry of Electronics and Information Technology, Government of India which wants to create an "Electronic Governance infrastructure" through:

- Aadhaar-Digital Biometric Identify infrastructure.
- GI Cloud (MeghRaj)
- State Wide Area Network (SWAN)
- E-Government Development Index (EDGI) under Global Indices
- Secure Email Service for Government of India
- Digital Locker
- Common Service Centers
- ETaal
- PRAGATI 2.0 : Pro-Active Governance and Timely Implementation
- Open Data
- Service Delivery Gateway

- Archive
- MyGov 2.0
- Government Procurement – Government e-Marketplace (GeM)
- State Data Centre
- Open Forge Project
- Jeevan Pramaan

PRIVACY AND ELECTRONIC GOVERNANCE IN INDIA

As Electronic Governance becomes an integral part of Government there is an increased sophistication in the maintenance of large databases and the primary area of privacy may be compromised. The overreaching question in the Indian context is the concept of data collection, use, disclosure, security and the anonymity with major reference to privacy in Electronic Governance. The data protection legislations have a central role for authorizing the use of personal and sensitive data. The primary safeguard for privacy and data protection requires consent from the stake holders and they should genuinely understand the potential risks that are associated with it. The existing data protection and privacy laws can be recognized and its ambivalence can be seen in *K S Puttaswamy v. Union of India (2017)*[6], where the Supreme Court of India recognized a "right to privacy inherent to the Constitutional right to liberty to be motivated by an imperative to assure the dignity of the individual"[7]. It was decided that privacy is intrinsic to the values of Article 21 which gives citizens the right to life and personal liberty and privacy should apply in both physical and technological form of information. For the individual to be guarded against State action which may be arbitrary the restriction imposed was to abide by the Article 14 and its exceptions to reasonableness.

In the Puttaswamy case the which was decided by a bench of the Supreme Court had a view that privacy and protection of data were complex issues and commissioned a report under the chairmanship of Justice B.N. Krishna, "*A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians",* submitted to the Ministry of Electronics and Information Technology, Government of India in 2018. The report considered that, first, 'the primary value that any data protection framework serves must be that of privacy' and second, 'such a framework must not

[6] K S Puttaswamy v Union of India (2017) 10 SCC 1

[7] 'Dignity is the core which unites the fundamental rights because the fundamental rights seek to achieve for each individual the dignity of existence. Privacy with its attendant values assures dignity to the individual and it is only when life can be enjoyed with dignity can liberty be of true substance. Privacy ensures the fulfillment of dignity and is a core value which the protection of life and liberty is intended to achieve': ibid (107).

overlook other values including collective values[8]. On the recommendation of the Committee it was suggested that a framework must be prepared to ensure data privacy and the processing and protecting of the data subjects shall be the sole responsibility of the data controllers who would now be given a new connotation as 'Data Fiduciaries'.

In regard to this it can be said that as meta data, machine learning and other techniques bring about a change in digital records and its maintenance, policy makers have to open the lines to keep and walk the thin line between large scale information which is digitized and may be personal along with the privacy norms that have been recommended by the committee of experts. In the Indian situation the data which is generated by its citizens who are called data providers is passed on to data users or collectors so that it may be used by public or private entities to provide services to their citizens.

The economics of privacy has become the major talking point as the data collectors for Electronic Governance in certain States of India has been handed over to private companies and in certain States, they are collected by the Government themselves. This data which is collected has an economic cost and, in an endeavor, to recover its cost there has been data pilferage.

The judgment in the Puttaswamy case has seen a statutory reform in the use of data which has now permitted private entities to use the Aadhar data in its biometric form[9]. This has opened the pandoras box as there are schools of thought which have differed on the use of Aadhar data by companies in the telecom space and the use of this data by banks. It has also brought the question of the use of personal information by these service-oriented organisations and after the use of the information the individual is entitled to the right to be forgotten.

GDPR – CONCEPTUAL COHERENCE WITH INDIA

The Data Protection Law which has been propounded in the European union is an ambivalent with regard to the central data protection safeguard. This law has moved in a direction to try and disconnect the right of privacy with right to data protection under the European law.[10] In the European Protection Law the Personal data is considered to be the data protection principles

[8] Committee of Experts under the Chairmanship of Justice BN Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Report to Ministry of Electronics and Information Technology, Government of India, 27 July 2018) 10 ('Protecting Privacy, Empowering Indians')

[9] The Aadhaar and Other Laws (Amendment) Act 2019. For commentary: See 'Lok Sabha Passes Aadhaar Amendment Bill', The Economic Times (online, 4 July 2019).

[10] Bart van der Sloot 'Legal Fundamentalism: Is Data Protection Really a Fundamental Rights?' in Ronald Leenes et al (eds), Data Protection and Privacy: (In) visibilities and Infrastructures (Springer, 2017).

which relate to lawfulness, transparency, accuracy, confidentiality and accountability are a part of GDPR and processing of data is determined as per the set of conditions that are propounded in Article 6 (1) of the GDPR.

A special mention should be made with regard to The United Kingdom Data Protection Law which has raised concerns on the privacy issues in governance and has recommended that various alternatives must be legitimized so that it demonstrates the power to substantive content. In the same Law the processing of personal data should be carried out by an established procedure under in the UK including the Data Protection Act, 2018 and the GDPR which is being applied through a processor or controller who for the personal data concerned in the UK context. Laws related to GDPR have certain additional protection under the Data Protection Law, through Article 9 of the GDPR. Under the new Data Protection Law, the privacy aspects with particular reference to Governance can be represented as:

- Consent and explicit consent are available for citizens on a lawful basis for processing.
- The concept of consent has been expanded through its recitals under GDPR with special reference to 32, 33, 157 and 171.
- If processing of data is done by an authorized body, then the said processing needs to be conducted to the same degree as required by Article 6 (e) of GDPR.
- The freedom of public bodies if they have a self-interest agenda is not allowed under GDPR.
- Automated processing should be left out to the discretion of individuals and the right not to subject to any form of decisions.
- Articles 44,45,46,47, and 48 have established that data transfer to a third country shall be through rules framed and not to undermine the Data Protection and Privacy Laws which are guaranteed under GDPR.

The conjoint of privacy interest depends upon the way in which the Government would like to implement e- governance and the rules of Information technology so that it can enhance the efficiency and ease for use by citizens and the privacy laws must be made in such a way that there is complete unanimity between the executive which is the law making body and the Government which implements the Electronic Governance projects.

The Indian Personal Data Protection Bill, 2019 has taken its main roots from the European Union GDPR and has recommended a trend of reliance on legal basis rather than legitimizing certain aspects of data privacy and protection. The expert committee has not looked into the test

of unfair processing along with the concept of valid consent which is discussed in detail under the GDPR. Free consent under the Indian Personal Data Protection Bill, 2019 is much lower when compared to GDPR and it is sufficient under Section 14 - Indian Contract Act of 1872 which that is only a sufficient clause and not an end in itself. The Indian Personal Data Protection Bill, 2019 has given significant protection than the European GDPR with regard to the use of term data fiduciary and has also made a significant contribution to the unequal bargaining positions of data controller and data principal. The Indian Personal Data Protection Bill, 2019 attempts to balance the Government on one hand and individual privacy in the collection of data so that this data can be used fairly and reasonably.

As the Government of India moves towards total Electronic Governance the challenges in the implementation of Electronic Governance can be described briefly as:

- Global constraints in the planning and decision-making process shall have an impact on Electronic Governance and digitization.
- Relevant laws, regulations and policies may sometimes limit the powers of the government complete Electronic Governance projects.
- Inter-State trade and commerce is always a challenge with regard to technical capability and also the different rules and regulations of the States and Union Territories in India.
- The digital divide between the citizens and business which are technologically complex and those who are against it may be a constrained for the Electronic Governance projects.
- As discussed, trust has been an important factor with citizens or businesses because of the laws that are prevalent in India and the accessibility of the Government to data .
- Data collection by the Government, maintenance of records and the use of information by the Government has always been a major hindrance and the same is to be addressed under Indian Personal Data Protection Bill, 2019.
- Security, data breaches, cyber-crimes have been especially high during Covid-19 and the Laws are not in place to guard Electronic Governance projects or websites.
- A recent issue is the online privacy which happens when two companies are merged with each other and the data of one company is transferred to other company without any contextual integrity.

If these disagreements are looked into under the new Data Protection Bill, 2019 it can be effective in promoting interests, moral and political values along with freedom.

CONCLUSION

It has been seen that Governments are implementing e-governance initiatives by incorporating technology, different stages of implementation of Electronic Governance to usher in paperless mode of bringing policies of the Government closer to the people. As meta data has increased Governments have to make capital expenditure for storage and retrieval of data. As the population of the day is increasing the availability of civic amenities has been an issue with local governments. In this regard electronic governance has to bridge the gap between use of data and providing solutions on a daily basis. India has confronted this dual challenge by integrating solutions through the India initiative announced by the Government of India on the digital front and is making an effort to improve the trust between Governments and citizens by promoting accountability, transparency and convenience in governance. There are certain questions which have been raised in Indian Law on the interpretation and application of 'fair and reasonable' in the case of Justice K.S. Puttaswamy v. Union of India, 2017. The apex Court in India in this case had very clearly indicated that ' data protection and information privacy is already a part of the right to privacy'. Different explanations have been offered to the right of privacy which have different implications but the main point is that laws in India which are both substantive in one sense and also procedural do not have any form of guarantees that can be offered on privacy in Electronic Governance. The risk of privacy and data protection were discussed in the paper under the new Data Protection Bill, 2019 whether data privacy was effective or ineffective in the current Electronic Governance norms. On the basis of the study concluded it can be said that in Indian situation and the hypothesis raised in this paper that perceived data privacy is ineffective in the current Electronic Governance norms. It is recommended that the Government bring into the proposed Indian Personal Data Protection Bill, 2019 to see that data processing on the basis of personal data in India with regard to Electronic Governance be made more informed and meaningful. Personal data protection must be taken for respect for individual rights and not an intrusion by the State to promote collective goals. Substantive safeguards if put into place on data privacy may help in Electronic Governance and if the interest of the citizens is protected then they would become a part of the Electronic Governance process which would be helpful in the rapid digitization of India. It can be said that if the Electronic Governance process in India has to succeed we should remember the words of the world-famous actor Marlon Brando "Privacy is not something that I am merely entitled to, it is an absolute prerequisite".