COMMENTS FOR WHITE PAPER OF THE COMMITTEE OF EXPERTS ON DATA PROTECTION FRAMEWORK FOR INDIA

BASIS THE NATIONAL CONFERENCE ON POLICY FRAMEWORK FOR DATA PROTECTION IN INDIA

HELD ON 22ND JANUARY, CONSTITUTION CLUB OF INDIA

The Dialogue
Inform Engage Ideate

Center for Knowledge Sovereignty

Bharat Niti

In association with

Microsoft

Policy Framework for Data Protection in India:

National Conference to Deliberate India's Data Protection Policy

22nd January 2018, 10:30am - 4:30pm
at Deputy Speaker Hall Annexe, Constitution Club of India, New Delhi

TABLE OF CONTENTS

1. BACKGROUND

Data is fundamentally transforming the way individuals do business, how they communicate, and how they make their decisions. Businesses are now building vast databases of consumer preferences and behaviour. Information can be compressed, sorted, manipulated, discovered and interpreted as never before, and can thus be more easily transformed into useful knowledge. The low costs of storing and processing information and the ease of data collection has resulted in the prevalence of long-term storage of information as well as collection of increasingly minute details about an individual which allows an extensive user profile to be created.

Recognising the importance of data protection and keeping personal data of citizens secure and protected, Ministry of Electronics and Information Technology (MEITY) constituted a committee of experts under the chairmanship of justice B.N Srikrishna, Former Judge, Supreme Court of India and comprising of members from government, academia and industry to study and identify key data protection issues and recommend methods for addressing them. the committee will suggest a draft Data Protection Bill. Protection of data is expected to provide big boost to digital economy of the country. In pursuance of the same, a white paper has been drafted to solicit public comments on what shape a data protection law must take.

The white paper outlines the issues that a majority of the members of the committee feel require incorporation in a law, relevant experiences from other countries and concerns regarding their incorporation, certain provisional views based on an evaluation of the issues vis-à-vis the objectives of the exercise, and specific questions for the public.

2. NEED FOR A COHERENT DATA PROTECTION LAW

Presently, Data protection in India is governed by loosely constructed provisions of the Information Technology Amended Act, 2008 (ITAA) under Sections 43-A and 72A of the Act. The effort to bring in a second legislation -- Personal Data Protection Bill -- governing data protection and privacy has been in the pipeline since 2006. In the digital age, privacy has become an intensely discussed and debated topic. In India with the privacy judgment and the ongoing Aadhaar case in the Supreme Court, a new public discourse has started around the issue of digital privacy. While data can be put to beneficial use, the unregulated and arbitrary use of data, especially personal data, has raised concerns regarding the privacy and autonomy of an individual. In order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a data protection law is the need of the hour for India.

3. NATIONAL CONFERENCE ON POLICY FRAMEWORK FOR DATA PROTECTION IN INDIA

In light with the growing importance of data protection and the white paper issued by the Ministry, Center for Knowledge Sovereignty, Bharat Niti and The Dialogue, with support from Microsoft, jointly delivered a one-day seminar titled "National Conference on Policy Framework for Data Protection in India", on 22nd January 2018. Mirror Now was the Knowledge Partner and contributed to the discourse with their inputs and views. This was an unprecedented development as media was involved as a stakeholder right from the pre-policy consultation. The Conference was held at the Constitution Club of India and was attended by approximately 120 people, who belonged to academia, government, consultancy as well as private and public sector professionals.

The following objectives were fulfilled at the conference:

- Generate a policy and legal discourse on data protection
- Take conversation forward on a proposed data protection law
- Gather comments to the white paper from high-level stakeholders to provide comprehensive suggestions to the ministry

The following broad themes were touched upon in the panel discussions that ensued lively debates and discussion leading to pragmatic suggestions:

- Definitions of personal data and sensitive personal data
- Jurisdiction and territorial scope of data protection laws
- Cross-border data flows and data localisation
- Exemptions to data protection law
- Notice and consent
- Big data challenge to privacy principles
- Processing of sensitive personal data
- Ensuring data quality
- New rights against discriminatory AI decisions, marketing, etc.
- Adopting a co-regulatory approach.
- Establishing deterrent consequences

In the report below, the discussions from the Conference have been summarised along with key inputs from Microsoft, The Dialogue and other stakeholders who participated at the event.

4. MICROSOFT’S INPUTS

4.1 PERSONAL DATA

- Requirements should apply to all data that is identified or identifiable to an individual, the same definition of “personal data” as under the GDPR and similar legislation worldwide.

- “Personal data” should be limited to data related to humans. Legal entities do not have the same rights in personal data as individuals and different laws should protect business data. Privacy rights should still apply with respect to the personal information of individual employees.

- Data protection rules that apply to the public sector should include meaningful restrictions on data processing to demonstrate that Indian law provides essentially equivalent protection to data protection laws in other regions to facilitate the free flow of data across borders. Appropriate restrictions on data processing by the public sector are also important for fostering the trust of foreign data subjects whose data may be accessed by the Indian government.

4.2 SENSITIVE DATA

- Additional protections to sensitive personal data should be provided and the level of restriction on the processing of personal data should correspond to the context in which the data is processed.

- The definition of “sensitive personal data” should be aligned to international norms, such as the GDPR

4.3 CONSENT

- The requirements for obtaining consent should be strong. A data protection law must sufficiently protect their interests, while considering their vulnerability, and exposure to risks online.

- Providing notice and obtaining consent at the point of data collection is at times either impractical or unnecessary. Individuals can be interrupted and overwhelmed if constantly presented with privacy choices and requests to collect data. In such instances, the "legitimate interest" legal ground for processing, which is incorporated into many global privacy laws, is vital for enabling companies to collect data that is necessary to support, deliver and improve a variety of services for the benefit of the data subject, controller or the society.

- The law should allow for the possibility of new purposes for processing previously collected data that may not have been knowable at the time of collection, but that are compatible with the original purposes of processing.

4.4 DE-IDENTIFICATION

Lawmakers should promote the use of data that has been subject to de-identification techniques that either eliminate or drastically reduce the ability to connect data with a specific individual.

4.5 RESPONSIBILITY

- It is important to maintain a distinction in responsibility between a data controller, which determines the means and purposes of processing data, and a data processor, which processes the data on behalf of another organization.

- A data controller should be primarily responsible for meeting privacy obligations and for providing redress to individuals. So long as a data processor merely processes data on behalf of a data controller its responsibility should be to follow its data controller's instructions and to assist the data controller in meeting its privacy and security obligations.

- Liability should be allocated among organizations that process data according to their demonstrated fault giving rise to the liability.

4.6 TERRITORIAL SCOPE

- National security is a legitimate motivation for accessing personal data and maintaining cross-border data flows are critical to preserving it. At the same time, compliance with international agreements, such as Mutual Legal Assistance Treaties (MLATs) is critical when data that raises specific privacy risks is to be shared with law enforcement organizations in third countries.

4.7 CROSS-BORDER DATA TRANSFER

- Indian law should facilitate intercompany and cross-border data flows that are protected through appropriate technical and legal measures and not otherwise prescribe the location of data.

- An effective approach is to adopt regulation that is interoperable with global standards or contracts that protect personal data regardless of its location. Such an approach can also help to improve resiliency and security and make data processing services more efficient by reducing latency. It will then be incumbent on data processing companies to make sure that the personal data that they process is managed according to local law, regardless of the location to which it is transferred.

- Bilateral or Multilateral Frameworks: Leveraging existing bilateral and multilateral frameworks would enable companies to use established principles and mechanisms to protect the privacy and security of personal data as it moves across borders. The EU-U.S. Privacy Shield, for example, offers a bilateral cross-border data transfer framework that could be a model for other jurisdictions.

5. THE DIALOGUE'S INPUTS

The Dialogue proposes a rights based data protection framework that drives innovation and entrepreneurship in India. A firm legal framework for data protection is the foundation on which data-driven innovation and entrepreneurship can flourish in India. Technology-specific language can get outdated quickly. Laws should be as technology neutral as possible. The benefits of cloud and artificial intelligence can only be fully realized once cloud infrastructure reaches a critical level of scale with global reach.

The law should mandate the consent of an individual for collection and processing of personal data. The final right to modify or remove personal data from any database, whether public or private, should rest solely with the individual. More importantly, the "exceptions" against this right should be defined narrowly, providing for a case-by-case consideration.

Data collectors and data processors should be differentiated and that they shall collect, store or access personal data in a lawful and transparent manner. Placing the issue of data security due to breaches on a higher pedestal, the data protection law should lay an obligation on data intermediaries to implement necessary security measures to ensure the security of data collected. Further, in case of a data breach, the law should ensure data intermediaries to inform individuals in a fixed time frame. It should also mandate the creation of an end user-facing position of data protection officer for grievance redressal, with a provision for appeal to the Data Privacy and Protection Authority (DPPA). This is undoubtedly one of the most important aspect, as it will allow individuals to file grievances against private as well as government bodies against any breach of privacy.

Lawful interceptions should have a list of exceptions, identifying a competent authority to approve such an act and defines the responsibility of state institutions involved in such acts.

All such acts would be under the purview of a data regulator and not under any ministry or judicial authority as seen under existing laws. The law should authorise data regulator to penalize, imprison and order compensation for losses suffered by individuals against private as well as government institutions involved in data collection or processing. However, it would be prudent that such tasks are assigned to other agencies as it may lead to a conflict of interest.

6. KEYNOTE SESSIONS

6.1 HEMANT GOSWAMI

Mr. Hemant Goswami, Chairman of Bharat NIti, gave the opening remarks of the conference and placed his ideas on the podium. He identified Aadhaar's ease and convenience to avail services, but also cautioned against its misuse.

Firstly, there are some third party enterprises involved and even with the best security infrastructure there will be gaps and they need to be understood and addressed. Secondly, a lot of transnational information sharing is happening and will increase and security will be difficult to address due to jurisdiction issue. He touched upon the need for data access for citizens and also highlighted the flow of data as it moves from different processors and controllers.

6.2 LT. GEN. DR. D.B. SHEKATKAR, PVSM, AVSM, VSM (RETD)

Lt. Gen. Shekatkar opened with a spiritual tone, identifying land, climate change, energy and water as all connected to data. For India to be aa global leader, he rightly pointed out on the need to generate and use data. We live in a border-less and blood-less world, where data is the new oil. It is therefore imperative that India knows the flow of data within and outside the country.

Everything is connected by data now. All the data generated in a country should primarily be used for the country in which it is produced. Times are changing. In 19th century it was all about muscle power, in 20th century it was all about money power and now in the 21st century it is all about knowledge power.

Countries are spending billions of dollars to spread knowledge about their prowess and India should acknowledge this opportunity, as we are living in the information age where knowledge governs everything.

6.3 VINIT GOENKA

Mr. Goenka started with important statistics on the role of data to drive industrial revolution and inter-connectivity spanning the key elements in our lives. By 2020, 50 billion smart devices will be activated.

The value of big data is close 26 billion USD. THe 4th Industrial revolution is currently happening, the era of big data and knowledge is upon us and development will be based on that and is already happening. Eg. Indian Railways and ISRO have signed an MOU where every single train is always tracked in real time. It is crucial to understand that Security nowadays is based on Data driven intelligence not human driven intelligence.

Firstly, period of data retention, there is a necessity to have a limit on the amount of time is data is held. Secondly Individuals and foreign nationals need to be included in the greater ambit of the report. Thirdly, we should build data centres in India and companies should use this infrastructure to store their data in India. It is about sovereignty due to the primacy of data, and for ensuring that India as an economy benefits from data-analytics.

Mr. Goenka provided some important suggestions to the Justice BN Shrikrishna Committee, which are as follows:

- Should add and define the word “individual”
- Data should be destroyed after its use
- Censorship – data sovereignty
- Data centres and servers should be within the borders

6.4 LT. GEN V.M. PATIL, PVSM, AVSM (RETD)

Lt. Gen. Patil opened his remarks with a cautionary tone of protecting data in the advent of digital economy. He gave examples of USA, EU and China, countries that have comprehensive data laws, an area where India is lagging behind. Ensuring the strength of the country needs very strong rules governing the strength of data protection. The current laws have been put in place with very limited knowledge of Information technology and computer science.

We also need to make a major and massive effort to include the bulk of the country into the internet. English currently rules the web and most Indians are left out because of that. Then the data information will increase a lot more, it is absolutely necessary to have data protection in place for them too.

The General Data Protection Regulation, developed by the EU, took seven years to be finaly drafted and has 32 countries as members. India faces both a challenge and opportunity to frame its own data laws with prior and comprehensive consultation with all key stakeholders. GDPR today is the most coherent data protection law and an example for India to follow.

Following are his suggestions to the white paper:

- Taking consent in the user's language
- Paperless, presence-less and cashless
- Data trust should be maintained
- Disclose data minimally to different data controllers according to its purpose
- Learned enterprises for audits(outside the governmental control)
- Consent brokers in case of dispute b/w individuals and organizations

Along with the above suggestions, he also noted individual's responsibilities, that are mentioned below:

- OS can be reinstalled but data is unique.
- Even computer and network can be protected
- Backup early and make it often
- Make file level encryption
- Password protect documents.
- Use EFS encryption
- Make use of public key infra
- IP security
- Secure wireless devices. Use mobile discretely
- Use right's management to retain control

7. PANEL 1: DISCUSSION ON DATA PROTECTION LAW AND IT ACT FROM LEGAL AS WELL AS TECHNOLOGICAL POINT OF VIEW

Speakers

1. Meenu Chandra: Senior Attorney, Microsoft India
2. Mukesh Jain: Chief Technology Officer, VFS Global
3. Deepak Maheshwari, Government Affairs Director, India and ASEAN, Symantec
4. BVL Narayana, Executive Director, CRIS, Ministry of Railways

Moderator

5. Kazim Rizvi, Founding Director, The Dialogue

The first panel discussion comprised of speakers from the corporate sector an the government, with the focus on the bird's eye view and key issues that should be included in the data protection framework going forward.

Mr. Mukesh Jain stated that individual defines their own understanding of privacy. TOS and app permissions are agreed and accepted without any consideration to their terms and people sacrifice most of their privacy due to them. If only 20% of consumers began to say no, companies would be forced to change the terms. But consumers are still being held hostage, people need to understand the power of saying no.

VFS destroys all consumer data within the one hour of final visa decision comes down. But most popular services online advertise personalisation capabilities and save user data for it and then go on and retain it indefinitely and abuse it. Only solution is to inculcate personal discipline especially for internationally based services.

But nationally we can push for better education on all issues plus reasonable policies need to be put in place. He had the following suggestion to make:

- Ethically wrong to deny a user if you deny permission/app access
- Cookies should not be allowed at all
- Start saying no when asked for your data
- In some cases, we might need personalization but not always

Deepak Maheshwari, in his remarks, called for a balance between different issues while fostering innovation. We need to have positive reinforcement for data controllers. The new data protection law should include prevention of fraud and law enforcement. Data transfers are multi-dimensional. In case of borders b/w two countries, bi-directional. EU GDPR – high fines, sanctions, enabling clauses such as notification/public notification in case of breach.

Meenu Chandra highlighted the need for implementing stating that it is one of the key concepts of privacy and data protection. Notification premise should be there by the company – to notify that this is the kind of data our company will use. She called for making MPLAD policies and law enforcement processes more efficiant. She also emphasised on facilitating cross-border data flow that follow similar standards to ISO Norms, European and American privacy rules.

Dr. BVL Narayana, CRIS, recognised an identity ambiguity in terms of who has the right to decide on what is the correction position. Access of data is an important area that should be addressed, while data centres should be maintained in India.

Data is now the identity and it is mandated for access to all services. Amendments to current status is absolutely necessary and the Shrikrishna report is a good start and deliberations are very important.

CRIS has its own rules which are mandated by the government, especially with regards to free access. The only identity check in the whole IRCTC process is when the TT on the train checks the ticket- anybody can book for anyone. There are central rules for sharing of data with Security agencies, cooperation is given freely. Big point of security maintenance is that there is CRISs own data centre where the data is stored. No rented servers and most importantly no using cloud computing for data storage which has many areas of potential data breach.

Dr. Avik Sarkar, OSD with Niti Aayog, emphasised on the need for data for developing robust policies and driving governance. India needs to usher into an era of designing policies on futuristic ideas such as AI etc. There is a lack of availability of good amount of training data for AI. While corporates take data for advertising purposes, we need to create an ecosystem that could prevent the misuse of personal data.

Following are a few additional suggestions made by Dr. Avik Sarkar:

Title: Liability of data lies with the data controller or the entity collecting the data at source

Comments are related to the two key terms described in the whitepaper: "Data Controller" and "Data Processor". According to the European Union regulation on personal data protection - "Data

Controller is the entity which determines the purposes and means of processing data" whereas, "Data Processor is an entity which processes data on behalf of the data controller".

The data controller either the entity collecting the information or regulatory agency on behalf of the data controller. Any data whether personal or private is collected for a particular purpose - this can be a business transaction like applying for a service, carrying out a medical check-up, withdrawing money from a bank account, etc. The citizen whose data we are referring to here, transacts with the entity, the data controller as the citizen completely trusts that entity. Since the information was shared on the basis of trust, the entity owning the data related to this transaction would be one and only one responsible for leak or loss of the underlying data.

The data controller might want to analyse the underlying data - either for non-monetary purpose like for improving service or for monetary purpose like sharing key trends, etc. In both these scenarios, the data controller may share the data with a trusted data processor under control environment such that there is no risk of the data been leaked or misused. Based on the above, the data controller is responsible for maintaining all confidentiality related to the collected data through the entire lifecycle of the data from collection till disposal.

Title: Sharing Data vs. Sharing insights

Data whether its personal or private may not be shared as it infringes upon the privacy of individual. Whereas insights from the data may be shared with interested parties for commercial purpose or non-commercial public good. Insights has to be derived from the data based on algorithms that help in discovering patterns from the data. It is good to clarify that discovering insights is not the same as calculating basic statistics from the data, but coming up with interesting patterns through the pattern of data mining. Raw data or simple aggregated data should not be shared in the form of insights. Experienced data scientists can deal with the process of discovering insights, which has to be taken on case by case basis. The data controller can share insights from the data that do not infringe upon the privacy of the people.

8. PANEL 2: ENFORCEMENT AND REGULATION FROM GOVERNMENT'S POINT OF VIEW

Speakers

1. Vinit Goenka, Member Governing Council, CRIS
2. Amit Dubey: Deputy Chief Technical Officer, Tech Mahindra
3. Jayadev Ranade, Member, National Security Advisory Board

4. Karma Bhutia: CEO, iShippo
5. Dr. Triveni Singh: IPS, UP Police

Moderator

6. Faye D’Souza : Editor, Mirror Now

Amit Dubey identified the challenge of identity theft and called for a robust data protection law based on the Indian system. He called for an intelligent system to determine ID theft and open source tools to combat fake news.

Mr. Jayadev Ranade, in his remarks, recommended that privacy should not only be in data collection, but also data storage. Data should be stored in Indian server and within the border. Mr. Vinit Goenka identified the need to have a data expiry date, and a law that needs to be reviewed periodically.

Dr. Triveni Singh recognised the insurance, car-purchase data that is already in the black market. He stated that data tamper, SQL injection, Fiddler are some of the tools that are used by hackers and anyone can learn them within an hour.

Karma Bhutia appreciated the architecture of Aadhaar, that is designed to give citizens an identity. The challenge lies with having third-party players, one of the reasons for leakages and breaches.

9. PANEL 3: INDIVIDUAL RIGHTS FROM A CITIZEN’S POINT OF VIEW

Speakers

1. Dr. Charru Malhotra, Indian Institute of Public Administration
2. Atul Tripathi, Cosultant, National Security Counsel Secretariat
3. Anand Krishnan, Senior Policy Analyst, Data Security Concil of India
4. Prof. Subhasis, IIT Delhi
5. Abhijit Chatterjee, Chief Innovation Officer, C-Zentrix
6. Puneet Bhasin, Lawyer

Moderator

7. Priyanka Chaudhuri : Counsel, Society Freedom Law Centre

Dr. Charru Malhotra acknowledged the importance of securing personal information nand identification. She questioned the surveillance aspect and asked, whether is it ethical to do state surveillance? Her recommendations to the white paper are as follows:

- Diversity should be integrated. Seniors, illiterates etc. Address the socio-cultural aspect.
- Consent and notice – Consent fatigue.
- Notice in what language. Or just a public notification?
- Data, when captured, as well as when stored, processed and in transition. How as a citizen can follow this pipeline and control the data?
- Data storage – servers should not be abroad. Increase the use of India’s sponsored services such as Digilocker and Meghraj cloud service
- Child consent – Is that the only subcategory we should be worried about? What about peasants and farmers? Australia and US defines child below 18 years
- Emerging technologies – do we really need a law like IT Act? This draft should be less of a law, but more of a framework covering AI, cryptos etc.
- Define minimum consent age
- Dashboard provision

Anand Krishnan, DSCI, noted that we need to shift from a consent-based system to a rights based system. He stated that the concept of notice is broken and T&C doesn’t really articulate the implications well. He highlighted the need for raising awareness about data protection across the country, and bringing the white paper into regional languages as well. Right to be forgotten has implications across the internet – individual should have the right to go online and delete its data sets. Following are some of his suggestions:

- Data relevancy needs to be understood more coherently
- Notice should be clear, unambiguous and in local language

Puneet Bhasin indicated that complete deletion of data in case of right to be forgotten may not be the right approach, but contextual and related data with related agencies should be deleted. She stressed on minor's consent, stating that the Indian contract act only focusses on 18 years+ audience. But child below 18 getting on internet and using FB, amazon and that's also a contract! It's a major glitch with child's consent. Can have a parental consent in addition to this.

- Responsible journalism – who defines this? Our framework only defines the word "responsible". It's subjective. Privacy should be well defined. Journalism is excluded, needs to be inclusive in the draft
- Privacy policy needs to be defined in the white paper
- Need of a data protection authority, but their role is very vague in white paper.

Mr. Atul Tripathi noted that social media has been the biggest trouble maker for police. He identified the need to get hold of data from social media.

Prof. Subhasis Banerjee, in his speech, stated the need to have virtual ID, along with the need to storing databases for profiling and investigative purposed.

He also pointed that data can only be used for pre-approved and legitimate purposes. Informational self-determination and the autonomy of an individual in controlling usage of personal data have emerged as central themes across the privacy judgment. It is argued that Indian data protection regime should offer stricter privacy protection than what is prevalent in the US, and on the other hand have a more innovation friendly setup than what the privacy protection framework in the European Union can offer, which perhaps is unduly restrictive without being commensurately effective. Additionally, the framework should be sensitive to our large under-privileged population which may not have the necessary cultural capital to deal with an overly complex digital setup.

A passive regulatory framework based on detection of privacy breaches, and traditional understanding of privacy protection based on the principles of consent, purpose limitation and transparency is unlikely to be successful for privacy protection. He also advocates an architectural solution based on online validation of authorisation and access control to prevent privacy infringements in the first place.