BLUE PAPER – CHARTING A NEW FRAMEWORK FOR DATA PROTECTION IN INDIA

*This Blue Paper is a result of a Roundtable discussion held on 4 September 2017, on the Discussion Document **Beyond Consent: A New Paradigm for Data Protection***

Prepared by:
Manasa Venkataraman and Ajay Patri

October 2017

ABOUT THE DISCUSSION DOCUMENT

This segment addresses the following aspects of the Discussion Document:

- *The foundational principles to govern any new data protection framework*
- *The salient features of the new data protection framework being proposed*
- *The key implementation features of the proposed framework*

Guiding Principles for Data Protection

Traditional models of data protection rely on an individual's consent to the terms and conditions of data processing. With the development of technology and an increased glut in information, this model is no longer feasible. The Discussion Document explores the possibility of an alternative to this model, one based on the principles outlined in this segment.

Accountability

An entity handling the data of an individual (a data controller) will be liable for any harm caused as a result of its actions. Consent, in such scenarios, cannot be a defense against liability.

Autonomy

The new model must be designed in a manner that ensures that an individual has the power to determine how much data he is willing to share.

Security

A data controller should be vested with the responsibility to ensure appropriate security standards are maintained with respect to the data.

Salient Features of the Proposed Model

Building on the guiding principles outlined earlier, the proposed model incorporates the following features.

Data rights

Every individual will have certain inalienable rights over their personal data.

Harm

The violation of the data rights will result in harm to the individual.

Liability

The causation of harm will make the entity handling the data liable.

Implementation Features

The implementation of the proposed model will be achieved through a combination of two entities: Learned Intermediary and Data Commissioner.

Learned Intermediary

A learned intermediary acts as an auditor, helping individuals and data controllers recognise biases in the system and suggest corrective measures.

Data Commissioner

A regulatory and adjudicatory authority that is also vested with the power to set standards for data protection.

ROUNDTABLE DISCUSSION POINTS

The Roundtable was chaired by Rahul Matthan, Fellow, Technology and Policy Research at the Takshashila Institution and Partner, Trilegal.

List of participants to the Roundtable:

- *Akash Mahajan, Co-founder, Appsecco*
- *Andrew Kramer , Omidyar Network*
- *Beni Chugh , Research Associate, IFMR Finance Foundation*
- *C. V. Madhukar, Investment Partner, Omidyar Network and Project Lead – Digital Identity*
- *Faiza Rahman, Consultant, National Institute of Public Finance and Policy*
- *Kiran Jonnalagadda, Co-founder, HasGeek and Internet Freedom Foundation*
- *Malavika Raghavan, Project Head for the Future of Finance Initiative at IFMR Finance Foundation*
- *Nayantara Narayan, Head of Policy and Research at the office of Mr. Baijayant 'Jay' Panda, Member of Parliament (MP) in the Lok Sabha*
- *Pranesh Prakash, Policy Director at the Centre for Internet and Society*
- *Sandesh Anand , Managing Consultant at Synopsys*
- *Subhashish Bhadra, Associate, Digital Identity, Omidyar Network*
- *Sukarn Singh Maini, Research Associate, Software Freedom Law Centre*

On Consent

Discussion Point #1: Agency of an individual

Consent allows an individual to maintain a certain level of control over his personal data. It empowers the individual to exercise his autonomy by refusing to deal with a particular data controller if he distrusts the terms on offer.

The corollary of this could also hold true, i.e., an individual might trust a data controller with his data despite the likelihood of a harm being caused. An individual should have the ability to judge such a scenario for himself.

Discussion Point #2: The threat of paternalism

A model that overrides an individual's consent might be construed as being too paternalistic. It would be symptomatic of a situation where the State claims to know what is best for the individual.

One must also consider the implications of this on the wider relationship between an individual and a State, particularly in a democratic nation.

On Consent

Discussion Point #3: A consent+ model

Given the shortcomings of consent and the importance of preserving an individual's autonomy, it could be worthwhile to explore a consent+ model.

Under this model, the accountability principle will become applicable in certain specified circumstances where it can be reasonably inferred that the individual has not consented to harm, or even the probability of harm. In all other situations not covered by this bare minimum threshold, the individual's consent will govern the relationship between the individual and the data controller.

Discussion Point #4: Feasibility of simplified consent

If the shortcoming of consent is that it is riddled with excessive legalese and jargon, one should also consider the possibility of having simplified consent mechanisms.

This would be akin to providing the individual with a privacy notice.

On Consent

Discussion Point #5: Scenarios where prior consent is not possible

The accountability model can also be applied in situations where prior consent of an individual cannot be obtained.

This could be seen in cases where data in the aggregate is converted to personally identifiable information. Typically, this conversion happens without the individual's consent being obtained.

Discussion Point #6: Data protection standards need not be universal

Given the vast differences in the use of data in various sectors, as well as the different levels of risks involved therein, it might be prudent to incorporate sector-specific standards of data protection. Under this, it is likely that consent might be overridden in some sectors where the likelihood of harm is high. Similarly, in other sectors, the consent of the individual will retain its primacy.

On Rights and Harms

Discussion Point #1: Institutional requirements

If the data protection framework relies on rights as the basis for protecting the interests of individuals, it must be accompanied by strong institutions capable of enforcing such rights. In the Indian context, it remains to be seen if the institutional capacity exists for handling such a framework.

Discussion Point #2: Gradation of rights

Apart from sectoral gradations in data protection, it could be useful to define various types of rights themselves. For instance, some rights could be classified as sensitive personal information or data. The thresholds for determining the harm caused due to the violation of such enumerated rights can accordingly be different.

On Liability

Discussion Point #1: The point in time when liability kicks in

It could be difficult to identify when a data controller becomes liable for its actions. For instance, in cases where an individual has been identified without his consent from disparate sources of data, would the mere identification, with the potential for future harm, result in liability? Or would there be a requirement for actual harm to be effected in order to ascertain liability?

Discussion Point #2: Determining who is liable for a harm caused

In most cases, the information belonging to an individual would have been within the control of various entities at some point of time before harm occurs. Given this, determining which of the entities involved is liable for the harm can be often difficult to pinpoint.

On Liability

Discussion Point #3: Liability for State actors

In order to be truly effective, a data protection framework must account for data rights violations by State actors as well. The definition of a data controller must necessarily include State actors handling the data of individuals.

One possible solution is to penalise the concerned department responsible for the violation by imposing a penalty that is a percentage of its budget. This would be in addition to any fines and compensation that other data controllers will be liable for under the law.

On Implementation

Discussion Point #1: Scope of audits

The information security model in India already incorporates elements of an audit, primarily through the nodal agency CERT-In. The efficacy of this model, however, is questionable. The audit requirements often do little in the way of improving security while increasing the complexity and cost of the systems being deployed. The inefficiencies of this model must be studied so that they can be avoided in the new framework.

Discussion Point #2: Cost of audits

Any requirement to conduct audits will come at a cost to data controllers. While this cost may not dent the finances of large corporations, it might inhibit the development of the start-up ecosystem in India.

Given this, it might be advisable to have graded levels of audit that are pegged to the size and finances of the data controller in question.

On Implementation

Discussion Point #3: Publication of queries

The model proposed in the Discussion Document provides for the publishing of queries that data controllers ask with respect to the individuals. Such queries can then be audited by Learned Intermediaries to identify patently bad actors. If implemented, it is unclear how this will be interpreted by enforcement authorities. There is a possibility that the content of the queries might conflict with the proprietary rights that data controllers have over their algorithms.

Having said that, it is easier to envisage a scenario where this can be made applicable to State actors.

Discussion Point #4: Composition of enforcement body

The enforcement organisation being contemplated should have the technical expertise to handle issues related to data protection. It would be advisable to avoid a body that is purely executive or judicial in nature.

On Implementation

Discussion Point #5: Ensuring compliance from data collectors

It would be worthwhile exploring the means by which data controllers can be encouraged to be more compliant with data standards. One option is the creation of a post of a Data Privacy Officer who can be made personally liable for violations that occur under his watch. Companies that appoint such officers have shown to be more cognizant of their responsibilities.

REFERENCE

Discussion Document:
Beyond Consent: A New Paradigm for Data Protection *by Rahul Matthan, Fellow, Technology & Policy Programme, The Takshashila Institution and Partner, Trilegal. Edited by: Manasa Venkataraman and Ajay Patri, The Takshashila Institution.*