RESPONSE TO

DRAFT PERSONAL DATA PROTECTION BILL, 2018

INPUTS FOR FORMULATING AN OVERARCHING DATA PROTECTION FRAMEWORK

Friday, 21 September 2018

RAJEEV CHANDRASEKHAR
MEMBER OF PARLIAMENT

Introduction

As India marches to its tryst with digitization under the Narendra Modi govts vision of Digital India, the importance of an overarching data protection framework to protect consumers rights can hardly be overstated. As someone who has argued for years in and out of the Parliament and litigated in Supreme Court for both Privacy and the related data protection rights, I have good reason to believe this. The Narendra Modi Government's recognition that the protection of personal data holds the key to empowerment, progress, and innovation needs to be appreciated and lauded.

I have been arguing and fighting for Digital consumer rights from some years ago – anticipating the situation that we find ourselves as a nation today of hundreds of millions of our citizens and businesses coming online. We are transforming into one of the world's largest digital/Data economies. I have taken my fights and arguments into and outside Parliament, including petitioning the Supreme court in a range of related issues like Sec66A, Aadhaar and Privacy as a Fundamental Right.

This effort is part of what I believe is a much needed framework for consumer rights – a Digital Magna Carta – a basket of legal consumer rights that include Data protection, Quality of service, Net neutrality, Free and Fair competition, Privacy etc.

The Srikrishna Report and the Draft Bill have made some progress in the endeavour towards an overarching data protection framework. The bill seeks to establish a fiduciary relationship between data principals (users) and data fiduciaries (data collectors and processors). The rights of the principals and fiduciaries are defined in the proposed law. The Srikrishna Report and draft bill have adopted various progressive goals such as anonymisation and legitimate interest processing.

The Srikrishna Committee Report is a good start. But the structural deficiencies in the draft bill however defeat these objectives. It also seeks the establishment of an omnibus regulator in the

form of a Data Protection Authority. Similarly, the extra territorial application of this prospective law will also cause many a conflict between jurisdictions globally. Finally, the bill proposes a broad-based clamp down on cross-border transfer of data.

Cross-Border Data Transfer

The restrictions on cross-border data transfers is likely to have far-reaching implications on India as an internet market. The draft bill requires that certain categories of data be stored in data centers located within India. These categories will be notified by the Data Protection Authority later. This requirement is likely to create a huge barrier to market entry given the enormous costs. India at present does not have the physical infrastructure to host large scale data centers. In addition to localisation, the bill requires contractual and inter-group cross-border transfer arrangements be approved by the Authority. This will significantly harm the ease of doing business given the dynamic business environment corporations function in today. These restrictions appear to be motivated only to facilitate law enforcement and Security agencies access to data and does not lead to any meaningful bolstering of privacy rights while it can be argued that the impact of such restrictions is also far reaching and disproportionate to the benefits.

The restrictions of on cross-border data transfers has the potential to create a case for isolating the Indian market. It is highly likely that countries such as the United States, under the Trump administration will respond kindly, in line with its terse stance on free trade. The great dividends of efficiency created by the internet will be lost to these measures that fragment it.

Data Protection Authority

The Data Protection Authority envisioned in the draft bill is likely to be the most powerful regulator in India till date. It has police powers such as search and seizure along with the powers to impose astonishing civil and criminal penalties. The Authority has sweeping rule-

making powers which makes the whole framework subject to the whims of the man on the wheel. Changes in data protection laws necessitates several consequential changes in network and storage infrastructure in addition to the very foundations of business models. The present proposals therefore are at the peril of establishing a vague and capricious regulatory regime. A better balance between privacy and highly intrusive and expensive regulation needs to be architected. The Srikrishna Committee Report recognises the critical principle of meaningful consent and also challenge of obtaining it. The threat of "consent fatigue" is real. The 'reasonable purpose' ground for processing however in the draft bill remains limited. The draft bill seeks to narrow these purposes in a manner that could threaten the entire purpose as an alternative to consent and future development that comes with innovation and processing albeit legitimately and not restrictively.

Anonymized Data

The Srikrishna Committee Report has proposed to exempt anonymised data from the data protection law. This is in line with global practice including the GDPR. The draft bill however adopts a standard of anonymisation that far surpasses the stringent standard in the GDPR. The bill requires "irreversible" anonymisation which is arguably technically impossible. Similarly, while carving out an exception for research activities is buried in red tape, as the bill requires specific approval of the Authority. Despite adopting a progressive outlook, the overarching objectives are frustrated.

Differential Compliance Framework Large Corporations and SMEs

The compliance framework proposed requires greater clarity. The draft bill adopts a differential approach for large corporations and SMEs dealing with data. Larger corporations dealing with a greater volume of data are subject to number of requirements such as audit and data protection impact assessments. The bill however does not clearly lay down this distinction which is likely to cause further compliance uncertainty.

Conclusion

The Srikrishna Committee Report and draft bill are an important juncture to closely examine the policy objectives that the government seeks to pursue with data protection. In addition to privacy, the government needs to be alive to the needs of creating a facilitative environment for business in India. The ideals of privacy and data protection in today's world will never be achieved by a regulatory bearhug.

Given the anomalies and contradictions the bill is laden with, rushing it to the winter sessions will be counter-productive since its ill planned and yet has wide reaching implications. So, this bill needs to be discussed thread bare for six months to a year beyond ICT companies, techies and lawyers. Its only then that the next stage of parliamentary intervention should begin.

Privacy and Data Protection are amongst the most critical parts of a Digital Magna Carta of consumer rights that are necessary for the long-term sustained success of Digital India. The proposed Data Protection law has many long-term implications and hence I recommend a more detailed and expanded discussion amongst all stakeholders before it is finalized.