Centre for Communication Governance
National Law University Delhi

Privacy Law Series

Towards a Data Protection Framework

- Chinmayi Arun and Smitha Krishna Prasad

This paper is a part of a series setting out our position on a data protection framework for India. All the papers in this series are based on our response to Committee of Experts set up by the Indian Ministry of Electronics and Information Technology for the implementation of data protection laws in India. Each paper is designed to break down our responses and position on the issues it addresses.

This paper sets out the context for the data protection law. It discusses the reasons and purpose for regulation and what specifically will be regulated. It also discusses who will be regulated, and discusses the regulatory strategies and legal frameworks to use while implementing the data protection principles.

Purpose of regulation

Arguably the immediate impetus for regulation in the form of a data protection framework comes from the Supreme Court's judgment in *Puttaswamy v. Union of India*[1]. However this judgment was delivered in the context of the (currently ongoing) litigation challenging the UID system, also known as Aadhaar[2]. This litigation has been accompanied by evidence

[1] Justice K.S Puttaswamy (Retd.) v. Union of India, (2017) 6 MLJ 267
[2] Justice K.S. Puttaswamy (Retd) and Anr. v. Union of India and Ors, W.P.(C) No.-494/2012 PIL-W; Our blog posts reporting on the final hearings in this matter are available at: https://ccgnludelhi.wordpress.com/tag/aadhaar-final-hearing/

gathering and activism, which continues as we write this[3]. This activism and evidence highlight additional reasons to regulate in public interest that may not be articulated in the Supreme Court's ruling in *Puttaswamy*. It is important to note these reasons, even though we focus on *Puttaswamy* and other legal principles arising from the Indian constitution and international human rights law in this paper.

The right to privacy is a fundamental right in India according to the Supreme Court of India's reading of the Indian Constitution.[4] This means that laws inconsistent with this fundamental right are not valid in India. Although the Indian Supreme Court has previously read privacy as a fundamental right in the context of state surveillance[5], press freedom[6], confidentiality in the context of medical information[7] and bodily autonomy[8], in *Puttaswamy v. Union of India* it articulated a broad definition of the right to privacy[9]. It is now clear that the right to privacy may be drawn from any of the other fundamental rights listed in the Constitution. Additionally, J. Chandrachud, J. Chelameswar, J. Kaul and J. Nariman have agreed that informational privacy is an important aspect of the right to privacy.[10]

The Supreme Court jurisprudence makes it clear that the data protection framework must enable individuals to exercise their fundamental right to privacy. It must be framed with the goal of protecting the right to privacy, especially informational privacy, of the people of India. The data protection framework must specifically protect the data and personal information of natural persons.

---

[3] Rachna Khaira, *Rs 500, 10 minutes, and you have access to billion Aadhaar details*, THE TRIBUNE, January 4, 2018, available at: http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html (Last visited on March 22, 2018); and Amber Sinha and Srinivas Kodali, *Information Security Practices of Aadhaar (or lack thereof): A documentation of public availability of Aadhaar Numbers with sensitive personal financial information*, THE CENTRE FOR INTERNET AND SOCIETY, May 1, 2017, available at: https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1 (Last visited March 22, 2018).

[4] Justice K.S Puttaswamy (Retd.) v. Union of India, (2017) 6 MLJ 267

[5] See PUCL v. Union of India (1997) 1 SCC 301 and Malak Singh v. State Of Punjab & Haryana (1981) 2 SCR 311

[6] See R. Rajagopal v. State of Tamil Nadu (1994) SCC 6 632

[7] See Mr. X. v. Hospital Z (1998) 8 SCC 296

[8] See the State of Karnataka v. Krishnappa AIR 2000 SC 1470

[9] Justice K.S Puttaswamy (Retd.) v. Union of India, (2017) 6 MLJ 267

[10] Justice K.S Puttaswamy (Retd.) v. Union of India, (2017) 6 MLJ 267 (this distinction is relevant since the judgment itself comprises of 5 concurring opinions author, with 4 being authored by the abovementioned judges. Justice Chandrachud's opinion has also been signed by the remaining judges on the 9 judge bench)

International law also recognises the right to privacy. India has accepted the applicability of the Universal Declaration of Human Rights (UDHR)[11] adopted by the United Nations General Assembly in 1948, and the International Convention on Civil and Political Rights (ICCPR) [12], and these International Conventions and norms are significant for the purpose of interpretation of the rights guaranteed under the Constitution. Both the UDHR[13] and the ICCPR[14] state that *'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation';* and that *'Everyone has the right to the protection of the law against such interference or attacks'.*

Other international norms and best practices are also emerging indicating an increasing need for adequate data protection measures to protect personal data[15].

In addition to the main purpose of regulation discussed above, it is relevant for the Indian business outsourcing industry to note that personal data from EU countries can only be transferred to non-EU countries that the European Commission declares as having an 'adequate' level of data protection[16]. This assessment examines, among other things, the extent to which data subjects can enforce rights against entities that process their data. It is therefore clear that it is also in the interests of the business outsourcing industry to put in place a strong and effective framework for data protection. If this framework is to be compliant with the GDPR, it must achieve the following[17]:

- Protection of individuals' personal data across dimensions of use
- Regulation of the use of such data horizontally, irrespective of the nature of the organisation / individual engaging in such use.
- Provide individuals with accessible remedies for any violations of their right to privacy and protection of personal data.

---

[11] UN General Assembly, Universal Declaration of Human Rights, 217 A (III) (Adopted on December 10, 1948)

[12] UN General Assembly, International Covenant on Civil and Political Rights, 999 UNTS 171 (Adopted on December 16, 1966).

[13] Article 12 of the UDHR

[14] Article 17 of the ICCPR

[15] For example, the standards set in various European Union data protection laws are now increasingly adopted in many jurisdictions outside the EU. See Graham Greenleaf, *'European' data privacy standards implemented in laws outside Europe*, (2017) 149 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT 21.

[16] Article 45, GDPR

[17] Report of the Group of Experts on Privacy, at 4.

Subjects of regulation

It would be difficult to craft an effective regulatory framework for data protection without understanding the subjects of regulation. The regulatory strategies used will need to work with the capacities, behavioural tendencies and incentives of those who are being regulated. We therefore discuss the targets of the data protection regulation in this part of the paper.

The law will need to apply to natural and juristic persons, public or private entities, who engage in the collection or use of data[18]. The first part of this is easy enough to understand – both individuals and corporate entities hold and process data, which means that the law will regulate both. The subjects may range from individuals collecting, storing and working with data, to small family owned establishment like the corner grocery shop that maintains lists of its customer's phone numbers and addresses, to a large corporation operating across a city, the country or globally. Without effective regulation of the private sector, the right to privacy cannot be meaningfully exercised. However, the private sector covers a range of players with differing capacities and resources. Attempts to regulate must take this into account.

It is equally important to ensure that the data protection framework extends to public entities, which are also very diverse in nature. It will be necessary to map and understand this in order to craft an effective and enforceable data protection framework for the public sector.

The nature of data held and controlled by public entities may be particularly sensitive, especially if combined, aggregated, or unlawfully accessed. Citizens are compelled to share data with the state to exercise various rights from getting passports to accessing health-care and their right to food and education. The state also accesses data originally shared with the private sector. State access to private information is sometimes transparent, in the context of employment laws for instance, but can be opaque in contexts like efforts by law enforcement agencies at surveillance of suspects.

[18] Centre for Communication Governance, *Comments to White Paper of the Committee of Experts on a Data Protection Framework for India*.

The Indian Supreme Court has recognized the applicability of informational privacy restrictions on the public sector[19] even before *Puttaswamy*. The AP Shah Report also notes that there is an international trend towards unified norms governing both the private and public sector, and argues that both should be covered by data protection law[20].

In addition to the applicability of the data protection framework to the public sector, it is necessary for the new data protection law to consider the effects of covert collection of data by the state, directly or via the private sector, on data protection. This would include state surveillance and law enforcement activities but would be broader and might extend to other kinds of opaque data collection. The state would therefore also need to be a subject of the data protection framework. This would necessitate an updation of the currently limited and inadequate regulation of state sponsored surveillance[21] but would also require the formation of new procedural safeguards within the data protection legislation.

A one-size-fit-all approach is as unlikely to be suitable for the public sector as it is for the private sector. It will be necessary to map and categorise the actors within both, and work out suitable strategies for both.

What is regulated

It is helpful to understand what is being regulated in the context of the object and purpose of the regulation. The new data protection framework should regulate the collection and use of any data that relates to an individual, whether an individual is identified or identifiable, directly or indirectly, and whether such data is accurate or not.

Collection and use of data can refer to a wide range of practices, some of which will emerge with new technology in the future. Different actors follow different practices: some engage in very traditional modes of data collection and storage such as making physical lists and locking them up; and others engage in sophisticated modes of collection, ranging from the use of third party applications to developing and using new technology. This means that the modes of collection and processing data increase as

[19] District Registrar & Collector, Hyderabad v. Canara Bank (2005) 1 SCC 496

[20] Report of the Group of Experts on Privacy, *available at* http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf (Last visited March 22, 2018).

[21] Chinmayi Arun, *Paper-Thin Safeguards and Mass Surveillance in India,* NATIONAL LAW SCHOOL OF INDIA REVIEW 26 (2014): 105 available at https://ssrn.com/abstract=2615958 (Last visited on March 22, 2018).

technology evolves. The data protection framework must accommodate both the traditional as well as the evolving ways in which data is collected, processed and stored.

In order to ensure that the data protection framework covers a wide spectrum of activities, the definition of personal information should be wide. The European Union's GDPR provides one example of the sort of wide definition that is necessary in this context: 'personal data' is simply defined as any information relating to an identified or identifiable natural person. The definition goes on to provide explanations regarding what might constitute identifiable information.

Given that data is increasingly transferred across borders for business today, the territorial scope of the law should also be carefully considered. The cross-border interaction fostered by the internet entails that India's data protection law must have a certain degree of extra-territorial applicability, in order to effectively protect the rights of residents and citizens. The Courts in India have similarly upheld the power of the legislature to enact laws with extra territorial reach, when "such extra-territorial aspects or causes have, or are expected to have, some impact on, or effect in, or consequences for: (a) the territory of India, or any part of India; or (b) the interests of, welfare of, well being of, or security of inhabitants of India, and Indians."[22] However, an overly broad and uncertain claim of extra territorial jurisdiction can create uncertainty for business, and impede economic activity, in a time when there is movement towards ensuring interoperable frameworks to promote cross border data flow. In that light, India should eschew articulations of uncertain scope. Restrictive practices such as mandatory data localization requirements should also be avoided.

Since a large amount of data already rests in public and private hands, the data protection legislation will also need to apply to data already in the possession of third parties.

Towards a Framework for Regulation

Before discussing the features of a regulatory framework for data protection, it is important to bear in mind that (as discussed above) the data protection framework is meant to protect the right to privacy, and that

[22] GVK Industries v. Income Tax Officer, 2011(4) SCC 36, para 76.

it aims to regulate the collection and use of data in this context. It is also important to consider the ecosystem which the framework will govern, and the wide range of individual and corporate, public and private, and Indian and international actors whose behaviour it will regulate. Taking this into account is likely to help us craft strategies that might ensure that the data protection rules actually influence the behaviour of all the actors that collect and use data. In this part of the paper we discuss some of these strategies.

We do not agree with the argument made in favour of a co-regulatory approach in the Committee of Experts' White Paper. This is because it poses risks of regulatory capture and domination by incumbent industry players with greater resources. Co-regulation will not only give industry leverage that civil society does not have, but will also disadvantage new commercial entrants with less capacity to engage with the regulator. This leads to two major risks – the first being that citizens may not be able access remedies when their right to privacy is violated; and the second, that innovation is affected because the incumbent actors have influence over the regulatory framework.

It is helpful to think of the framework in three broad stages – setting standards, monitoring and enforcement. Our discussion above of what is regulated will be key to rule formation. However, the standards must be framed such that they are as consistent with the goal of regulation as possible. Later in this series of papers we discuss what standards might be ideal to begin with for a data protection law in India. Towards this end, the GDPR, and work by data protection scholars has proven useful both substantively and towards ensuring that India's norms are easier to comprehend owing to the use of shared language.

In addition to standard setting, it is important to bear in mind that the interpretation of the standard, monitoring and enforcement play a major role in ensuring that the standard is actually observed. The data protection framework must come with proactive monitoring by the data protection authority as far as possible. It must also offer consumers and users adequate access to redressal mechanisms. These redressal mechanisms must account for the fact that industry often has deeper pockets than consumers and must be architected to offer actual access to individuals whose rights have been violated.

In the interests of accountability, an independent data protection authority must be created, with adequate resources and powers to administer the

data protection law. We discuss the accountability framework and the use of principles of 'responsive regulation' later in this series. In addition to the data protection authority we recommend strengthening accountability frameworks across the law, leveraging the expertise and power of sector specific regulators.

A complex system of this nature should be constructed through multiple rounds of consultation, and the involvement of multiple independent experts. It should also feature review mechanisms that allow for consultation and course-correction at regular intervals.