Centre for
The Digital Future

White Paper

Legal Framework
for
Privacy In India

Revisit – Reframe – Revise

March 2022

Legal Framework for Privacy in India
Revisit – Reframe – Revise

1. Introduction

While upholding the right to privacy as a fundamental right within the constitutional framework of India in 2017[1], the Supreme Court had recommended a robust legal regime for data protection while recognizing that ***"Informational privacy is a facet of the right to privacy"***.

Over the past decade, the focus of the legislation-in-making has indeed shifted from the broader concept of **'Privacy'** to **'Data Protection'**. All the same, it is pertinent to mention that while taking note of the Government's move to architect a data protection framework, the Supreme Court neither precluded nor advocated legislation for **'Privacy Protection'** *per se***.**

It follows from the SC ruling that, a **'Data Protection'** law would at best deal with just one facet of **'Privacy'**. In fact, the **Data Protection Bill, 2021 (DPB, 2021)** recommended by the **Joint Parliamentary Committee (JPC)[2]** further restricts the scope to digital data only and that too held by private entities, with state entities largely being either exempted or exemptible from its ambit[3].

Considering the substantive shift in the scope and ambit of the proposed law, it is imperative to undertake open public consultation afresh in line with the **Pre-Legislative Consultation Policy, 2014[4]**. Such an endeavor would help refocus the Bill more appropriately, smoothen the rough edges as well as enhance clarity, consistency, and certainty while allowing requisite flexibility.

As noted in the SC plurality judgment, it needs ***"a careful and sensitive balance between individual interests and legitimate concerns of the state"***. In addition, it should foster an enabling and conducive environment for data fiduciaries to innovate in a free and fair competitive market.

2. Data Protection ≠ Privacy

Notwithstanding the long history of discussions around privacy within the Parliament and existence of several legal provisions pertaining to specific aspects of privacy, India has no dedicated privacy legislation. Coinciding with the commencement of **Aadhaar[5]** enrolment process in 2010, the government had indeed initiated consultations on a privacy law but made little progress[6].

---

[1] https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
[2] http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1
[3] http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf
[4] https://legislative.gov.in/sites/default/files/plcp.pdf
[5] https://uidai.gov.in
[6] https://documents.doptcirculars.nic.in/D2/D02rti/12AUGUST.pdf

Subsequently, in line with its terms of reference[7], a committee of experts chaired by **Justice B N Srikrishna** proposed the **Personal Data Protection Bill, 2018 (PDP Bill, 2018)[8].** Thereafter, the government introduced a modified version as the **Personal Data Protection Bill, 2019 (PDP Bill, 2019)[9]** in the Parliament and it was referred to a **Joint Parliamentary Committee (JPC)** leading to the recommendations mentioned earlier.

Logically, data protection norms should be a derivative of and predicated on the privacy framework and not the other way around. However, the widely held but fundamentally flawed view is that the proposed '**Data Protection'** legislation is India's '**Privacy'** legislation.

3. Guiding Principles

Privacy itself is an evolving societal value and hence, not amenable to elaborate codification. This is why the SC explicitly and consciously chose not to embark on any such codification. But if the data protection emanates from the privacy framework, what is the way forward?

In its essence, the **Right to Privacy** empowers one to exercise agency and choose if and what about them can be learned or gleaned by others, when and how; and, furthermore, if and how the same can be used or shared with a third party.

Accordingly, the legal framework for privacy must be predicated not on an elaborate codification of what constitutes private information, but on certain clear, consistent and easy-to-apply principles. Further, the 'Right to Privacy' should neither be predicated on, nor be circumscribed by any specific technological or business process context *per se*. Such an egalitarian approach would future-proof the law obviating the need for frequent amendments necessitated by constant evolution of technologies and business models.

In 2012, a group of experts chaired by **Justice AP Shah** had recommended a set of nine principles for operationalizing privacy by way of a legislative framework[10]: Notice; Choice and Consent; Collection Limitation; Purpose Limitation; Access and Correction; Disclosure of Information; Security; Openness; and Accountability.

Incidentally, similar principles find place in all the three legislative drafts not only in India (2018, 2019 and 2021) but also in most other jurisdictions and frameworks, giving them a sense of universality. Hence, the law must explicitly lay down and enshrine such principles.

4. Data Protection Perspective

Even from the limited perspective of **'Data Protection**', the Bill raises significant concerns beyond those already mentioned above. These include but are not limited to the following:

---

[7] https://www.meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf
[8] https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
[9] http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
[10] https://niti.gov.in/planningcommission.gov.in/docs/reports/genrep/rep_privacy.pdf

4.1 Non-Personal Data In, Non-Digital Data Out

The **JPC** recommended renaming the Bill from '**Personal Data Protection'** to **'Data Protection'** arguing that the blurring boundaries between personal and non-personal data (the latter including anonymized personal data) necessitated a single overarching legal instrument.

Curiously, the **JPC** narrowed the scope to **'digital protection'** only thereby proffering no protection in the proposed law from harm emanating from misuse of data in non-digital form. If the lines between the **'Personal Data'** and **'Non-Personal Data'** are blurring, **'digital data'** and **'non-digital data'** have always been fungible.

Hence, logic dictates that the 'Data Protection' legislative framework must include data and information in the non-digital realm.

4.2 The Missing Indian Context

Successive DP Bills in India have been largely modelled on **European Union's General Data Protection Regulation (EU GDPR)**[11]. However, the privacy law must take into cognizance the socio-cultural context and political economy of India that are both very different from Europe.

India is digitizing at a rapid pace and has a vibrant and burgeoning start-up eco-system. Additionally, it needs to protect the global leadership and competitiveness of its world renowned IT-BPM sector.

GDPR may be appropriate for Europe, but even there, its adverse impacts are becoming visible. These include but are not limited to 'consent fatigue' and 'innovation constraints'.

Hence, the legislation must be better tailored to the Indian socio-cultural milieu and its political economy.

4.3 Exceptions and Exemptions for Government Agencies

Being a fundamental right privacy is first and foremost justiciable against infringement by the state. While upholding privacy as a fundamental right, the Supreme Court had also laid out certain preconditions that must be met where incursions into individual privacy might be permissible, albeit under narrowly crafted and clearly laid down exceptions.

Such actions must comply with the just, fair, and reasonable procedure mandated under the Article 21 of the Constitution as well as pass the triple test of legality, legitimacy, and proportionality prescribed by the Supreme Court of India.

[11] https://gdpr-info.eu

Considering that 'public order' is the very first entry in the List II of the Seventh Schedule thereby giving exclusive legislative powers to the state governments in this realm, any power exclusively vested with the central government might conflict with the constitutional doctrine of division of powers between the union and the states.

Hence, the exceptions and exemptions for government agencies must be narrowed down to agencies tasked with national security, intelligence, and law enforcement only and that too, with judicial or parliamentary oversight.

Moreover, such powers should be vested with the 'appropriate governments' for the respective subject matters under their jurisdictions listed within the Seventh Schedule, albeit only for the reasonable restrictions in accordance with the letter and spirit of the Article 19(2).

4.4 Just, Fair, Reasonable and Proportionate Norms

As noted by the Supreme Court, privacy has both positive and negative connotations and has both a normative and descriptive function. Being contextual and dependent on ever-evolving societal norms and buffeted by continuing rapid technological developments, hard codification of privacy is neither possible nor perhaps, even desirable.

Admittedly, in the context of empowering the executive to exempt a government agency from all or any provisions of the law under clause 35, the procedure followed must be just, fair, reasonable, and proportionate. **Likewise, the same set of tests should also guide all the stakeholders ascertain the contours of data protection norms under particular context.**

4.5 Data Classification

The Bill classifies data into two broad categories as **'Personally Identifiable Information'** (**PII**) and **'Sensitive Personal Information'** (**SPI** includes data pertaining to healthcare, sexual orientation, religious or philosophical beliefs, etc.) besides vesting the powers with the central government to notify any particular type of data as **'Critical Data'**.

However, such hard classification of broad categories of data can lead to unnecessary complications. For example, though health data has been classified as **SPI**, the potential harm from a disclosure of someone being HIV positive would be very different from a disclosure of someone running a temporary, low-grade fever.

However, data classification should be left to the discretion of data fiduciaries subject to the principles laid down in law and their being accountable to justify their decision.

4.6 Adverse Impact of Compliance Burden on Start-ups and Innovation

Limitations inherent in the techno-centric focus on '**Data Protection'** amplify the compliance burden on data fiduciaries, without any commensurate benefit towards ensuring or enhancing **'Privacy Protection'** of individuals.

While large and established businesses might arguably be able to comply with such elaborate mechanisms, start-ups and MSMEs would bear its crushing brunt and may suffer early mortality, even if as an unintended consequence.

Over-reliance on consent itself may be counterproductive. Socio-economic disparities, lower literacy levels and enormous diversity across languages and scripts within India add further complexity. The state needs to lay down a certain minimum level of privacy that it is best placed to enforce, rather than leave it as the subject matter of an asymmetrical negotiation between a mighty data fiduciary and a powerless individual even if called data principal through a consent mechanism that only amplifies the underlying and inherent inequality.

Worryingly, the legally sanctioned **'Consent Managers'** may emerge as the new brokers. In the same manner, seeking fresh consent for every new purpose would add unnecessary friction for users and retard innovation for providers.

Instead, reuse should be allowed for any purpose that is compatible with, or not materially different from, the original one as is allowed even under the **EU GDPR** and in the **California Consumer Protection Act (CCPA)**[12]. Likewise, hard data localization would also increase costs and limit choices coupled with possible degraded services.

Hence, rigorous Regulatory Impact Assessment (RIA) must be undertaken to evaluate the rationale, need and impact of such provisions on individual privacy as well as on businesses, especially start-ups and MSMEs.

4.7 Social Media Intermediaries as Publishers

The proposed Data Protection framework goes on to treat the social media companies as publishers thereby making them accountable for unlawful user generated content and take away the safe harbor protection they enjoy under the extant law.

Irrespective of the merits and demerits of this proposition, it is noteworthy that such action has no direct nexus with data protection at all and hence, totally out of place and context. This amounts to diluting the core focus and thrust of the principal law while setting an undesirable precedent, likely driven by expediency of the state.

Accordingly, the provisions pertaining to classifying social media companies as publishers should be excised from the DPB, 2021.

[12] https://oag.ca.gov/privacy/ccpa

Any change in the law or rules pertaining to intermediary liability for user generated content, however, may be undertaken during the proposed review of the **Information Technology Act, 2000**[13].

5 The Way Forward

The need of the hour is to **revisit** the legislation-in-making in its entirety and ensure that the **'Right to Privacy' reclaims** its legitimate primacy and focus therein. The law needs to lead with clear privacy principles. Only essential features of data protection that follow from those principles need find place in the principal legislation with details relegated to the Rules.

This will impart requisite agility, flexibility and longevity to the legal framework obviating the need for frequent amendments. A wider consultation is a must to **revise** it accordingly.

About Centre for The Digital Future

Centre for The Digital Future (CDF) was launched on October 30, 2019 with a vision to conduct actionable research on the impact of digitisation on the economy and society. The inquiries are analytical, without any pre-determined bias, multi-dimensional and evidence-based, and provide policy and regulatory insights that enable the transition to an optimal digital economy and society.

The Centre has been established and incubated as an entity by the **India Development Foundation (IDF)**, a private non-profit research organisation set up as a Trust in 2003.

For more information, please visit https://cdfresearch.org or https://idfresearch.org.

[13] https://www.meity.gov.in/content/information-technology-act-2000