Looking Beyond Individual Privacy: Limits of Personal Data Protection in the Face of New Harms

www.iconnectblog.com/looking-beyond-individual-privacy-limits-of-personal-data-protection-in-the-face-of-new-harms/

I•CONnect March 19, 2026

—Sukriti and Palash Srivastava, Centre for Communication Governance, NLU Delhi

India released its Digital Personal Data Protection Rules (‘Rules’) in November 2025, and is now poised for the enforcement of its Digital Personal Data Protection Act, 2023 (‘Act’). The fundamental basis of data protection laws (in India and elsewhere), including the Act, is premised on the idea of individual control over personal data enabled through the notion of ‘informed consent’. The concept of informed consent, embodied specifically in Section 4, 5 and 6 of the Act read with Rule 3 of the Rules, implies that data may be

collected and processed only after seeking consent of the user or the data principal after providing adequate notice containing information regarding the purpose of collecting their data.

In view of the wide ranging forms of big data and the proliferation of algorithmic processing of data, this post investigates whether traditional data protection regimes are effective in tackling emerging concerns regarding privacy and data protection, with a focus on India's data protection approach.

Why Legacy Personal Data Protection Approaches Fall Short

Under the Indian Act, personal data are defined as "any data about an individual who is identifiable by or in relation to such data." Here, data is defined as "representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means." Although this definition may be interpreted broadly, the scope seems to be restricted to data that identifies an individual. This may result in the negation of inferences possible through sophisticated and expansive forms of algorithmic data processing (including Big Data processes) and mass data collection, derived from mixed data sets containing both personal data (relating to an individual) and non-personal data (which might be in aggregate form). Such processing of data is conducted on a wide scale to draw inferences at the level of large populations to arrive at patterns and group profiles, which can in turn be utilized to inform general policies applied at scale. Predictive technologies built on machine learning and Big Data can combine large amounts of sectoral metadata, aggregate data, and other forms of collective data, enabling inferences that may be arrived at without necessarily processing data with information that contains personal identifiers. For example, a 2020 ethnographic study on Delhi Police's predictive policing system revealed that data on the frequency of emergency calls and crime, mapped with pre-existing historical bias, led to self-reinforcing 'hotspots' where policing of marginalized communities was intensified, even in the absence of any personal data collected.

Such processing of data can in turn reinforce biased or discriminatory profiling or decision-making, and thus invade privacy. Professor Sandra Wachter has explained how online platform providers, such as Facebook and Google, through behavioral advertisements, can infer sensitive information about users who are targeted or excluded from products, services or offered differential pricing based on their inferred profile.

In the current paradigm of personal data protection in India, individuals hold little control and oversight over how their data is evaluated upon processing, and have little to no recourse against inferences being drawn from their data. Traditional notions of consent that form the basis of data protection laws fail to account for these inferences that may lead to egregious privacy violations.

For instance, consent is required for “processing of personal data for the specified purpose and limited to such personal data as is necessary for such specified purpose.” However, the above-described privacy risks are not dependent on personal data collected in the manner envisaged by the Act through an idea of notice and consent based data sharing. Moreover, most of these privacy risks are not individual-centric, but rather, arise from the algorithmically created groupings and affinities of an individual in comparison with and alongside others, and the consequent profiling.

While traditional data protection approaches, like that embodied in the Act, operate within a limited frame of individual personal data collection limited to a specific purpose, advanced data processing techniques infer substantial details about an individual not by reliance on personal data or individual identification, but through a combination of different data points such as those obtained from user’s online activity, pre-existing data, and/or data scraped from the web. In addition, where consent for the processing of personal data was given prior to the Act’s commencement, the data fiduciary can continue processing the data until the data principal withdraws their consent. Moreover, under section 3(c), the Act is inapplicable for personal data made publicly available, such as on social media sites. This leaves much of the digital footprint left by individuals unprotected, particularly in view of increasing instances of mass data scraping. This renders the traditional concepts of data fiduciary (defined under the Act as, “any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data”), data principal (defined under the Act as, “the individual to whom the personal data relates), and purpose limitation, obsolete and redundant, or at best applicable very narrowly. Combined with the narrow definitional ambit of personal data, much of the data collected as part of the large data processing described above will likely fall outside the scope of personal data, and the consequent processing of such data will remain outside the realm of the data protection law.

Previous Policy Developments

India has previously relied on regulatory and policy considerations that were based on the idea that a strict binary of ‘personal’ and ‘non-personal’ data is inadequate for privacy protection. For instance, the Draft Data Protection Bill 2021, which was the result of recommendations of the Joint Parliamentary Committee, governed both personal and non-personal data. A 2020 Report by the Committee of Experts on Non-Personal Data Governance Framework had recommended the establishment of a Non-Personal Data Authority to factor in considerations of group privacy. However, it did not include details on how to operationalize it. Similarly, the Draft Data Use and Accessibility Policy (2022) proposed a framework for economic uses of non-personal, public sector data “for catalyzing large scale social transformation”, but did not include any considerations for privacy protection. Subsequently, the Draft National Data Governance Framework Policy (2022) failed to examine privacy harms arising from reidentification of anonymized data and from the combination of various data sets. India has not witnessed any new policy developments on the subject since. Notably, these draft policies came before the entry into force of any data protection law in India. In fact, one of the initial proposals for

economic uses of data came from the Economic Survey of 2019 which suggested the government could monetize data for public good by giving the private sector paid access to data sets. This suggestion received criticism at the time for inadequate privacy considerations in the absence of a data protection law.

Need for Alternative Approaches to Data Protection

In response to the structural limitation of personal data protection, there is a growing body of scholarship proposing alternative frameworks and regulatory solutions that address systemic, inference-driven and group-level risks.

Since the inferences drawn from the processing of data are often at the level of groups with shared interests or traits, or from a combination of non-personal and personal data, 'group privacy' is a concept devised to overcome the limitations of individual-centric notions of privacy and personal data protection. Basu and Sinha note, 'we are increasingly being confronted by a world where critical decisions about and for us made by data driven systems are dependent as much on choices made not just by us but others who belong to the aggregate and conglomerate collectives that we are a part of.' Group privacy enables protection for groups that are more vulnerable to targeting, and where a lawfully processed set of personal data may be used to arrive at inferences at a group level. This concept approaches 'groups' in two different ways – firstly, pre-existing social categories like gender, age, and caste which create additional vulnerabilities in many contexts even when identifiable data from an individual has not been collected; and secondly, as ad hoc groupings created by algorithmic filters and inferences drawn from various data points. These two 'groups' often converge, where algorithmically created groupings often act as proxies or correlate to pre-existing societal axes of oppression and marginalization.

In India, the landmark case of *Puttaswamy*, which affirmed the fundamental right to privacy, arguably places a positive obligation on the State to ensure the conditions for privacy protection as opposed to purely a negative right to be invoked against specific instances of overreach by the State. The judgment notes that the state should enable the formulation of adequate policy measures beyond personal data protection. Furthermore, the standard of consent envisioned by the judgement is that of *informed* consent, i.e. the information must be collected only after consent *and* "…used for the purpose and *to the extent it was disclosed*". On close reading, it is clear that the Court envisioned privacy not merely as a formalistic 'right against interference' but as a more holistic *control* over one's information, decisions and self-expression.

The understanding of privacy furthered by the Court in *Puttaswamy* provides the theoretical and jurisprudential foundation for expanding data protection beyond its current individualistic conceptualization. A full expression of one's identity is not possible in a scenario where one is constantly subjected to decision-making by increasingly opaque algorithms. Additionally, informed consent is reduced to its mere form since an individual is incapable of knowing what 'groups' one would be algorithmically placed in and how decisions with respect to these categories would be made. Thus, for a

meaningful realization of the Supreme Court's vision of privacy, a promising way forward could be a conceptualization of group privacy that widens the prevailing individualistic understanding of the right to privacy for meaningful data protection and enforcement. This would require a further development of the theoretical and jurisprudential threads in *Puttaswamy* or a fundamental rethinking thereof, which could be achieved by scholarly contributions, a judgment by another court, or a new policy/governance framework such as those attempted previously in the context of non-personal data.

Additionally, emerging frameworks for AI-enabled data processing could be instructive for India, specifically when it comes to introducing privacy-protecting approaches to data processing. Under those frameworks, the legality of processing depends not only on the nature of data collected but also on the *purposes*, *contexts*, and *impact* of the inferences drawn from it. The EU AI Act, for instance, classifies AI systems by risk and imposes heightened obligations for high-risk and inference-heavy uses, including mandatory Algorithmic Impact Assessments, documentation of datasets and model behavior, fairness testing, and post-deployment monitoring. To mitigate discriminatory profiling, the EU AI Act also requires independent algorithmic audits, conformity assessments, and clear prohibitions on harmful uses such as social scoring or exploitative predictive analytics.

By reopening its stagnated discourse around non-personal data and by considering a risk-based governance framework for AI-enabled data processing, India can ensure that its regulation is alive to the privacy risks in the contemporary AI landscape.

Finally, a potential approach could be to develop a 'right to reasonable inferences', which could be understood as a positive manifestation of pre-existing right to privacy under Article 21 and right against arbitrariness under Article 14 of the Indian Constitution. Proposed by Wachter and Mittelstadt, this right understands grouping as a limit upon autonomy and inaccurate grouping as a violation of autonomy in itself. It requires entities using algorithmic models to justify why certain data provides a valid basis for drawing inferences, why the inferences are normatively appropriate for the decision at hand, and whether the methods used are reliable. Triggering this requirement should not be dependent upon an individual having to show harm as a consequence of being grouped inaccurately, but would rather be a disclosure that entities must mandatorily provide, prior to any data processing.

Together, these regulatory and technical interventions move beyond the narrow scope of personal data protection and recognize that modern AI-driven data ecosystems require systemic safeguards capable of addressing inference-based, aggregated and group-level harms that traditional data protection laws cannot capture. It overcomes the limitations of individual consent and the narrow scope of personal data and its processing within the Act and the Rules, and enables a realistic accounting of the prevalent and dominant risks to privacy.

Suggested citation: Sukriti and Palash Srivastava, *Looking Beyond Individual Privacy: Limits of Personal Data Protection in the Face of New Harms*, Int'l J. Const. L. Blog, Mar. 19, 2026, at: http://www.iconnectblog.com/looking-beyond-individual-privacy-limits-of-personal-data-protection-in-the-face-of-new-harms/

Sukriti works as a Project Officer at the Centre for Communication Governance at National Law University Delhi (CCG). She is interested in data protection and privacy, platform governance, and issues of digital rights and free speech. Palash works as an Analyst at the Centre for Communication Governance at National Law University Delhi (CCG). He is interested in platform regulation, artificial intelligence and human rights issues in the context of emerging technologies.

Next PostThe Mexican Judicial Reform: An Illustration of a Discrepancy in the Literature ›

Leave a Reply

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.