THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

November 4, 2026

Data Protection Act: Consent Cannot Replace a Proportionality Test

By: Subhashis Banerjee

The consent of an individual cannot meet the test of proportionality in an intrusive state scheme. But India's data protection act does not require a test be made as the Supreme Court set in Puttaswamy. An independently reviewed proportionality analysis should be made before data collection.

India's Digital Personal Data Protection Act, 2023 (DPDP Act) was meant to give legal form to a constitutional promise. In *Justice K.S. Puttaswamy v Union of India* (2017), a nine-judge bench of the Supreme Court held privacy to be a fundamental right under Article 21 of the Constitution. It did not stop at declaring the right. The leading judgment laid down how any intrusion by the state must be tested. There must be a law, the law must pursue a legitimate aim, and the intrusion must be proportionate to that aim.

> The question worth asking is whether the Act does what Puttaswamy required. On the central test, proportionality, it does not.

Proportionality asks three questions. Can the measure achieve its purpose (suitability)? Could a less intrusive alternative achieve it adequately (necessity)? Do the benefits justify the infringement of rights (balancing)? A useful purpose alone is not enough. Justice Sanjay Kishan Kaul added that there must be procedural safeguards against abuse. The court also urged the government to enact a data protection regime that would meet these standards.

Consider, for example, the electoral bonds case decided by the Supreme Court in 2024. The government argued that allowing political donations through banks while concealing donors' identities would help curb unaccounted political funding and protect donor privacy. The court examined whether the scheme could advance these objectives (suitability), whether less restrictive alternatives could achieve them without similarly compromising voters' right to information (necessity), and whether the restriction on that right could ultimately be justified (balancing). It found that less restrictive alternatives, including electoral trusts, were available. Having concluded that the scheme failed the necessity test, the majority did not need to undertake the final balancing exercise and struck it down.

What followed took six years. The Srikrishna Committee's 2018 draft bill borrowed heavily from the General Data Protection Regulation (GDPR). The 2019 bill widened state exemptions. It was withdrawn in 2022, after a joint parliamentary committee review. The 2023 act is a far leaner text. The DPDP Rules were notified in November 2025, with most of the main duties scheduled to take effect in May 2027.

The question worth asking is whether the DPDP Act does what *Puttaswamy* required. On the central test, proportionality, it does not.

The issue is not simply whether particular provisions of the act, or schemes operating under it, would survive constitutional scrutiny. It is whether the law places a duty on institutions to demonstrate proportionality before intrusive data processing systems are deployed.

Two Designs

The DPDP Act is built around consent. A data fiduciary (the body that decides how and why personal data is processed) may process personal data with the data principal's (the person the data relates to) consent. It may also do so for one of a closed list of "certain legitimate uses" in section 7. For private actors, that list is narrow, so consent does most of the work. For the state, the list is generous.

> Proportionality is a condition of lawful processing, assessed before the data is touched.

Section 7(b) covers subsidies, benefits, and services that the government prescribes, subject to conditions. These concern earlier consent or data held in notified government records, and the applicable processing standards. It permits the present processing without fresh consent; earlier consent may satisfy one condition.

Section 7(c) covers functions "under any law". It also covers processing in the interest of the sovereignty, integrity or security of the state, and for that part it does not expressly require a separate enabling law. Constitutional requirements still apply. Section 17(2)(a) lets the government exempt notified state bodies from the act on specified grounds. None of these provisions requires a test of necessity or proportionality.

The GDPR starts somewhere else. It treats data protection as a fundamental right under the Charter of Fundamental Rights of the European Union. Consent is only one of six lawful bases for processing, and the right one depends on the processing. The key difference is where proportionality sits.

A public authority performing its tasks must point to a law that is clear, foreseeable, and proportionate to its aim (Article 6[3]). It cannot rely on legitimate interests when performing those tasks. A private controller (the GDPR's term for a data fiduciary) that relies on legitimate interests must first show necessity, and then balance its interest against the data subject's (the data principal's) rights. High-risk processing requires an impact assessment that weighs necessity and proportionality (Article 35). In each case, proportionality is a condition of lawful processing, assessed before the data is touched.

Left to the Courts

The word "proportionality" does not appear in the DPDP Act. The act does not generally require the state to publish an assessment, before deploying a processing scheme, showing that the scheme is necessary and comparing less intrusive alternatives.

> Without mandatory advance documentation and scrutiny, citizens may have to discover and challenge a database, a data linkage, or an exemption themselves.

Data fiduciaries that the government designates as "significant", a category that may include state bodies, must carry out periodic assessments, subject to exemptions. But this is not a general mechanism for independent constitutional scrutiny in advance. The Data Protection Board is appointed by the central government, and it has no advisory role on legislation or executive notifications. It rules on breaches of the act's specific duties after they occur.

The act therefore relies on accountability after the event. A fiduciary is to give notice and take consent where required, keep data secure and report breaches, and the board can penalise failures. This design does not repeal the *Puttaswamy* test; it simply leaves it out. The constitutional obligation to justify an intrusion already binds the state, and it does not begin with litigation. But without mandatory advance documentation and scrutiny, citizens may have to discover and challenge a database, a data linkage, or an exemption themselves.

Courts can review proposed measures as well as existing ones. But court rulings of this kind cannot substitute for a duty on institutions to publish and defend the justification before deployment.

Compliance Is Not Harm Accountability

Imagine a bank refuses someone a loan after using a profile assembled from several databases. A regulator can check whether the bank followed the rules for collecting and processing personal data, and penalise it for any violations, even if no one suffered demonstrable harm. But what if the bank complied with all these rules, yet rejected the application because of an invalid inference, drawn from the combined data by artificial intelligence (AI)? Establishing that the inference was invalid-and holding the bank accountable for it-would be much harder.

> The Act provides penalties for non-compliance, but no compensation under its own framework; the penalties go to the state.

Two kinds of accountability must be distinguished. Compliance accountability asks whether a fiduciary violated a duty under the act. A regulator can establish a failure to give notice or keep data secure without proving injury to any individual. Harm accountability asks whether particular processing caused an adverse consequence.

With personal data, the chain of cause and inference is often invisible. Someone denied a loan, flagged for a welfare investigation, or targeted by a scam may never discover which linkage, inference or disclosure contributed to the decision. Harms may surface months

later, elsewhere.

The act provides penalties for non-compliance, but no compensation under its own framework; the penalties go to the state. Processors (bodies that handle data on a fiduciary's behalf) are regulated mainly through fiduciaries, and outsiders may be unable to see the relevant data flows. Crucially, even perfect enforcement of the duties on notice, consent, and security cannot show that a scheme that otherwise complies is necessary or proportionate.

The Dutch SyRI and childcare-benefits scandals show how problematic profiling systems may need scrutiny by courts, journalists and civil society. Enforcing compliance is indispensable, but it cannot substitute for scrutiny of the processing itself.

Consent Is Not Authorisation

Three questions must be kept separate. Is this use of data justified? Who may access which data, and for what operation? Has the person validly agreed?

Legitimacy asks whether processing for a stated purpose is justified by law, necessity, and proportionality. The legal test that applies depends on the actor and context. Authorisation asks whether a particular actor may access particular data for a particular operation, under a policy that can be enforced and audited. Consent asks whether an individual has validly agreed, where agreement is an appropriate legal basis.

> A welfare scheme, a health record or an identity system should rest on a specific law that states its purpose, its data, and its limits.

Consent may feed into authorisation, but it cannot establish legitimacy. Nor does authorisation alone establish legitimacy. A consent record specifying "loan underwriting" does not show that every item of data requested is necessary. Nor does it control all later inferences and linkages. A system can comply with the consent rules yet be disproportionate, or be legitimate in purpose yet insecure in how access is controlled.

Over-reliance on consent also ignores the conditions in which it is obtained. Individuals rarely know what linked data can reveal, and they have little power to negotiate terms. When consent is effectively the price of a loan or treatment, formal agreement may conceal coercion. The GDPR explicitly scrutinises imbalance of power and the conditioning of a service on unnecessary processing. The DPDP Act requires free and specific consent, but it has no equally developed framework for assessing such imbalances of power (Solove 2013).

For public services, the point is sharper still. A welfare scheme, a health record or an identity system should rest on a specific law that states its purpose, its data, and its limits. It must not violate people's rights even if they consent. Consent cannot make a disproportionate scheme proportionate. Hiding behind consent is not a principled option.

Proportionality Before Deployment

The alternative is to do what Puttaswamy asked, and to do it before deployment. Every significant or intrusive state processing scheme should be supported by a written, published proportionality analysis before it goes live. The analysis would state the purpose and the law that authorises it. It would show that the system can actually achieve the purpose, and set out the less intrusive alternatives considered. It would also specify what data is collected, who can access it, which systems it is linked to, and for how long it is kept.

> Private high-risk processing should also undergo proportionate, risk-based review, irrespective of consent.

A body independent of the department proposing the scheme should review the analysis. Private high-risk processing should also undergo proportionate, risk-based review, irrespective of consent. This is a proposal for statutory governance. It does not claim that every private use of data without consent directly attracts the constitutional test for state action.

Consider a hypothetical proposal to link public health records across hospitals to detect outbreaks earlier. The assessment would identify the authorising law. It would require evidence of improved detection over existing reporting, perhaps from a limited pilot measuring detection times, missed cases, and false alerts.

It would compare linkage with aggregate reporting, with collecting fewer data fields, and with analysis within hospitals that shares only alerts. It would specify the records and identifiers needed. It would assess the risks of mistaken matches, sensitive disclosures, and unrelated reuse, and identify who bears them. It would restrict identifiable access to authorised health staff, and specify access logs, encryption, retention limits, and correction procedures. It would then justify the remaining risks against the evidenced benefits. If the evidence were inadequate, the scheme should be narrowed, redesigned or withheld.

Publication matters as much as the analysis itself. A published assessment can be contested before harm occurs, rather than reconstructed in court afterwards. It gives the Board and the courts a record against which to test later conduct. Above all, it turns the state's existing constitutional burden of justification into a duty it must meet before deployment.

Regulation Does Not Block Innovation

It is tempting to dismiss proportionality analysis before deployment as regulation standing in the way of innovation. "Innovation versus regulation" is a false choice. A design that cannot contain the harms it creates is not particularly innovative. It simply shifts its costs onto the people whose data it processes.

Proportionality analysis asks designers to state what a system is for, to show that it works, and to find the least intrusive way of achieving it. These are design questions, and answering them well is what good engineering looks like. The two can, and should, go hand in hand (Cohen 2013).

A Dutch assessment of Zoom illustrates how scrutiny can improve design. After identifying excessive data collection and other privacy risks, the assessment prompted negotiations that led to changes in the software, retention rules and access controls. Zoom also redesigned its business statistics so that European users' data were aggregated in Europe before statistics were transferred to the United States. The service continued, with less intrusive processing.

Proportionality Needs a Grammar

Proportionality is necessary, but it does not apply itself. In the Aadhaar judgment (2018), the majority and Justice D.Y. Chandrachud's dissent applied the same test to the same scheme and reached opposite conclusions. The majority weighed the benefits of deduplication and minimal data collection, and found the scheme proportionate. The dissent weighed the exclusion caused by biometric failure and the surveillance structure the scheme created, and found it unconstitutional.

> Claimed benefits need measurable outcomes and evidence that the system actually works.

The GDPR's enforcement record-more than two thousand fines, running to several billion euros-also shows that legal duties and controllers' own compliance assessments do not guarantee lawful processing.

The lesson is that benefits and risks must be stated in a precise, common language. Claimed benefits need measurable outcomes and evidence that the system actually works. Risks need explicit threat models, the effects of linking datasets, error rates, and an account of who bears them. Without such a grammar, proportionality analysis becomes rhetoric, and whoever controls the narrative controls the outcome.

The framework is right. Putting it into practice requires a precise way of stating risk. Developing such a grammar, and a way of testing the evidence behind proportionality claims, is the subject of a future article.

Subhashis Banerjee is a professor of computer science at Ashoka University, Sonipat. He also leads the Centre for Digitalisation, AI and Society.

References:

Cohen, Julie E. 2013. "What Privacy Is For." *Harvard Law Review* 126 (7): 1904-33. https://harvardlawreview.org/print/vol-126/what-privacy-is-for/

Nas, Sjoera, and Floor Terra, with assistance from Jacob Gursky. 2024. Update DPIA Zoom Education. Public version, April 3. *Privacy Company*, commissioned by SURF, especially pp. 156-159. Report.

Solove, Daniel J. 2013. "Introduction: Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126 (7): 1880-1903. https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/