IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Whose Algorithm, Whose Consent? Rethinking India's Consent Manager Framework through the Lens of Datafication and Constitutional Equality

1Somya Srivastava, 2Dr Saif Ali Khan

1Assistant Professor, 2Assistant Professor

1Integral University,

2Integral University

Abstract

India's new data protection law, the Digital Personal Data Protection Act of 2023, and its 2025 Rules, create a new kind of intermediary called the Consent Manager. The idea is that instead of every individual having to deal separately with hundreds of companies that collect their personal data, a single registered platform will let the user give, review, manage, and withdraw consent across all of them. This article examines whether the design of the Consent Manager will actually work for ordinary Indians, particularly those who are poor, less digitally literate, do not read English or Hindi well, share their phones with family members, or live in remote areas. It traces the legal architecture of the Consent Manager through the DPDP Act and the 2025 Rules, compares it with the existing Account Aggregator framework in the financial sector, and tests it against the constitutional standards of equality and proportionality laid down by the Supreme Court of India. The argument is that the present design assumes a data principal who is literate, English-speaking, smartphone-owning, and individually situated. Most data principals in India are not all of these things. The article concludes with five concrete reforms that can be brought in through delegated rules and regulatory guidance, without amending the Act itself, to make the Consent Manager genuinely accessible to the populations it most needs to protect.

Keywords Consent Manager · Digital Personal Data Protection Act 2023 · DPDP Rules 2025 · Algorithmic governance · Vulnerable populations · Account Aggregator · Privacy self-management · Constitutional morality

1 An intermediary in search of a subject

The Digital Personal Data Protection Act, 2023 (hereafter DPDP Act) arrived in the Indian statute book bearing the rhetorical weight of two decades of constitutional, technological, and political ferment. Following the Supreme Court's affirmation of informational privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1, three legislative drafts, multiple expert committees, and a sustained civil-society campaign, the statute was assented to in August 2023 and operationalised through the Digital Personal Data Protection Rules, 2025, notified by the Ministry of Electronics and Information Technology on 13 November 2025 (MeitY 2025). Among its more distinctive features is the introduction of a new regulated intermediary, the Consent Manager, defined in section 2(g) of the DPDP Act as a person registered with the Data Protection Board of India who enables a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. Conceptually, the Consent Manager is an institutional artefact of what Indian policy literature has come to call the Data Empowerment and Protection Architecture (DEPA), an inter-operable framework first piloted in the financial sector through the Reserve Bank of India's Account Aggregator system in 2021 (Reserve Bank of India 2016; Sahamati 2023). The premise is intuitively attractive: instead of leaving the individual to navigate hundreds of opaque privacy policies and click-wrap interfaces, a regulated intermediary will mediate consent on her behalf, recording each grant and withdrawal in a cryptographically verifiable ledger and shuttling data between fiduciaries through a data-blind transport layer. The Indian Government has presented this model as a uniquely Indian contribution to global data governance, an architecture in which, as the official communications repeatedly emphasise, the user is sovereign (MeitY 2022).

This article subjects that promise to critical scrutiny from the vantage point of AI & Society's editorial preoccupation with the way algorithms shape, and are shaped by, the cultures in which they are deployed. The journal has insisted that the analytical centre of gravity must shift from algorithmic governance shaping society to society shaping the algorithm (AI & Society, Aims and Scope; Gunkel 2023). On that test, the Consent Manager fares poorly. Its design assumes a data principal who is literate in English or Hindi, comfortable with smartphone-mediated dashboards, capable of comprehending the temporal and informational consequences of granular consent flows, and willing to delegate the management of those flows to a private intermediary subject to a registration regime that imposes substantial barriers to entry. The lived realities of a country in which only thirty-eight percent of rural and semi-urban users meaningfully comprehend the digital products they use (Policy Circle 2025), in which roughly forty percent of the population speaks neither English nor Hindi as a first language, and in which the largest single use-case for digital identity and digital payments remains welfare disbursal to economically marginal households, sit in awkward tension with that design vision.

The argument advanced here is not that Consent Managers are unworthy or destined to fail. It is more pointed. The institutional choices reflected in the 2025 Rules, in particular the minimum net-worth requirement of two crore rupees, the prohibition on dual roles, the data-blind transport mandate, the seven-year retention obligation, and the absence of any duty to design for low-literacy users or for the twenty-two languages recognised by the Eighth Schedule of the Constitution, encode a particular socio-technical imagination. That imagination is one in which the data principal is presumed competent, the intermediary is presumed neutral, the fiduciary is presumed compliant, and the regulator is presumed effective. Each of these presumptions is contestable. Together, they risk converting an instrument that was meant to liberate the individual from the burdens of privacy self-management into one that further entrenches the structural asymmetries it claims to dissolve.

The article proceeds in five further sections. Section 2 reconstructs the Consent Manager framework as it stands after the November 2025 notification, locating it in the DEPA lineage and tracing the journey from the 2018 Srikrishna draft through the 2019 Personal Data Protection Bill to the 2023 enactment. Section 3 sets out the theoretical scaffolding for the critique, drawing on Solove's consent dilemma, Nissenbaum's contextual integrity, and Zuboff's surveillance capitalism, and adapting these to the Indian

setting. Section 4 turns to the empirical realities of vulnerable populations, examining digital literacy data, linguistic diversity, the experience of the Account Aggregator framework, and emerging evidence on dark patterns in Indian consent interfaces. Section 5 develops the constitutional argument, drawing on Puttaswamy, Anuradha Bhasin v. Union of India (2020) 3 SCC 637, and Puttaswamy II (Aadhaar Five-Judge Bench, 2018) to argue that the present design falls short of the proportionality test and the equality guarantee. Section 6 proposes a set of reforms, framed around the journal's call for society shaping the algorithm: differentiated user-interface obligations, mandatory linguistic accessibility, an independent grievance ombudsman, restrictions on dark patterns, and a re-orientation of the regulator's mandate towards substantive rather than merely procedural compliance. Section 7 concludes.

2 The architecture of the Consent Manager

2.1 Statutory provenance

The Consent Manager first surfaced in the Indian policy lexicon in the Justice B.N. Srikrishna Committee Report of July 2018, which recommended a framework of consent-based data sharing intermediaries inspired by the Account Aggregator model then under development by the Reserve Bank of India (Government of India 2018). The 2019 Personal Data Protection Bill carried the concept forward as a category of data fiduciary tasked with enabling consent management. The 2022 Digital Personal Data Protection Bill, which followed the withdrawal of the 2019 Bill, narrowed the definition. The 2023 Act, in its final form, retained the figure as a registered intermediary but left most operational details to delegated legislation.

Section 6(7) of the DPDP Act provides that the data principal may give, manage, review or withdraw her consent through a Consent Manager and that the Consent Manager shall be accountable to her. Section 6(8) requires registration with the Data Protection Board of India and adherence to such technical, operational, financial and other conditions as may be prescribed. The remaining detail was supplied by Rule 4 and the First Schedule of the DPDP Rules, 2025, which the Government notified, after a public consultation on the draft rules of January 2025, in the Gazette of India of 14 November 2025 (Ministry of Electronics and Information Technology 2025).

2.2 Registration, capital, and capacity

Part A of the First Schedule prescribes the eligibility conditions. The applicant must be a company incorporated in India. It must demonstrate a minimum net worth of two crore rupees, adjusted annually for inflation. It must satisfy the Board of the technical, operational and financial capacity to discharge its functions. Its directors and senior management must possess a credible track record of integrity. Its constitutional documents must explicitly embed its DPDP obligations, and any amendment to those documents requires prior approval from the Board. An independent certification is required to confirm that its interoperable platform meets prescribed data-protection standards (Ministry of Electronics and Information Technology 2025; Tsaaro 2025).

These provisions construct a high entry barrier. The two-crore-rupee threshold, roughly equivalent to two hundred and twenty-five thousand United States dollars at prevailing exchange rates, excludes the bulk of civil-society organisations, public-interest technology collectives and grassroots digital-rights groups that might otherwise have offered context-sensitive consent management to vulnerable users. The structure inevitably privileges well-capitalised commercial entities, several of which have already signalled an intent to enter the market (MediaNama 2025). The framework's stated rationale, that only entities with adequate financial standing can be trusted to manage consent on behalf of millions of data principals, is reasonable on its face; its distributional consequences, however, deserve closer attention than they have so far received in the regulatory discourse.

2.3 Functional obligations

Part B of the First Schedule sets out the functional obligations of the Consent Manager. It must operate an interoperable, user-facing website or application; it must record consents and the privacy notices preceding them; it must route both the consent and, where applicable, the requested personal data to the transferee fiduciary; it must use a data-blind transport layer so that it cannot itself read the contents of the data package in transit; it must facilitate data portability either directly or through the source fiduciary; it must provide a single dashboard for the data principal to review historical consents, modify them, or withdraw them granularly at any time; it must respond to grievances within ninety days; and it must maintain consent records, in machine-readable form, for at least seven years (Ministry of Electronics and Information Technology 2025; AZB & Partners 2026).

Several features are noteworthy. First, the data-blind transport architecture, derived from the Account Aggregator playbook, is genuinely protective: a Consent Manager cannot, in principle, read or repurpose the data that passes through its system. Second, the prohibition on dual roles ensures that an entity cannot simultaneously act as a data fiduciary or processor for the same data principal whose consent it manages, addressing at least the most obvious conflict of interest. Third, the recordkeeping obligation creates an evidentiary trail that, in theory, would assist the regulator and the data principal in disputes about whether consent was in fact obtained, withdrawn, or relied upon. These design choices reflect a careful technocratic sensibility and have been welcomed by the legal and consulting community (Bass Berry Sims 2026; Lexology 2025).

2.4 What the architecture presupposes

Yet for all its technical refinement, the architecture presupposes a particular user. That user owns a smartphone with reliable internet connectivity. She is comfortable navigating multi-step authentication flows. She understands the abstract distinction between a data fiduciary, a Consent Manager, and a data principal. She has the time, the cognitive bandwidth, and the inclination to review historical consents on a dashboard. She is sufficiently literate to read notices in either of the official languages, or in whichever languages a particular Consent Manager chooses to offer. She trusts a privately incorporated intermediary, supervised by a regulator whose composition is dominated by executive appointees, to act in her interest rather than that of the fiduciaries who pay for the privilege of plugging into its platform. None of these presuppositions is uniformly true in India. They are most untrue for the populations the framework most needs to protect.

3 The theoretical inheritance: consent, contextual integrity, and the political economy of platforms

3.1 The consent dilemma

The most thorough indictment of consent-based privacy regulation remains Daniel Solove's analysis of what he termed privacy self-management (Solove 2013). Privacy self-management, Solove argued, asks individuals to bear a burden they cannot meaningfully discharge: the cumulative cognitive demand of reading, understanding, and weighing the consequences of every consent decision exceeds the capacity of even the most diligent user. Drawing on empirical work showing that reading the privacy notices encountered by an average internet user in a single year would require more than two hundred hours (McDonald and Cranor 2008), Solove concluded that meaningful consent is structurally unattainable within the notice-and-choice paradigm. He returned to the theme a decade later, observing that successive regulatory generations have responded to the failure of consent by demanding more consent, producing what he now calls murky consent: a regulatory fiction that legitimates collection while serving no protective function (Solove 2024).

Nissenbaum's contextual integrity offers a complementary diagnosis from a different theoretical register. Privacy, on her account, is not the control of personal information in the abstract; it is the appropriate flow of information according to the norms of the social context in which it is generated and circulated (Nissenbaum 2010, 2011). What is appropriate in a medical context is not what is appropriate in a commercial one; what may flow between friends may not flow between an employee and an employer. The Indian Consent Manager, in seeking to abstract consent decisions from their substantive contexts and channel them through a generic dashboard, replicates precisely the contextual flattening that Nissenbaum identified as the source of widespread informational dissonance.

Zuboff (2019), writing within yet another tradition, situates the contemporary failure of consent within the political economy of surveillance capitalism. Consent, on her analysis, has become an instrument by which platform power is legitimated rather than constrained. The asymmetry between the individual user and the platform is so vast, and the platform's interest in extracting behavioural surplus so structurally entrenched, that consent functions as ritual rather than authorisation. These three theoretical lenses, while distinct, converge on a single proposition that bears directly on the Consent Manager debate: a regulatory framework which delegates the substantive protection of privacy to individual choice, however well-mediated, will fail in proportion to the social, cognitive, and material asymmetries within which those choices are made.

3.2 The consent-intermediary turn and its limits

Consent intermediaries are not an Indian invention. Lehtiniemi and Kortesniemi (2017), drawing on European MyData experiments, examined whether the structural obstacles to privacy self-management can be overcome through the introduction of a trusted third party that aggregates consent decisions, simplifies interfaces, and acts as the user's agent in negotiating with data controllers. Their conclusion was cautiously optimistic but heavily caveated. Consent intermediaries can reduce the search and comprehension costs that burden individual users; they cannot, however, dissolve the underlying power asymmetries, and they introduce a new principal-agent problem of their own. If the intermediary is funded by the data controllers it negotiates against, its incentives are skewed. If it is funded by the user, the model is unlikely to scale to populations that cannot pay. If it is funded by the State, it becomes another node of state surveillance. The Indian Consent Manager, on present design, leans towards the first model: although Rule 4 forbids revenue generation from data sharing itself, intermediaries are expected to recover costs through fees levied on participating data fiduciaries (Sahamati 2023; AZB & Partners 2026). The structural risk that Lehtiniemi and Kortesniemi flagged is therefore alive and unattended.

3.3 Datafication and the production of vulnerability

A further conceptual move is needed before the Indian setting can be diagnosed with precision. Mejias and Couldry (2019, 2024) have argued that the contemporary moment is best understood not as the protection of pre-existing privacy interests against a new technological threat, but as the constitution of new social subjects through datafication. Vulnerability, on this account, is not simply a pre-political attribute that some populations bring to data interactions; it is, in part, produced by the data interactions themselves. The rural welfare beneficiary, the gig worker, the migrant labourer, the adolescent on a feed-curated social platform, the woman in a household where the smartphone is shared and the credentials are not hers, each become legible to the data economy in ways that aggregate, sort, and re-distribute their access to credit, opportunity, and recognition.

When the Indian regulatory imagination presents the Consent Manager as the user's tool, it implicitly invokes a liberal individualist anthropology in which the user is a coherent, autonomous, choosing subject whose decisions about her data are her own. The empirical data principal in much of India occupies a more contingent social position. Her smartphone may be borrowed; her aadhaar may be linked to a relative's bank account; her welfare entitlements may be conditional on consent flows she does not

control. To presume otherwise is to reproduce, in the law of data protection, the very abstractions that have made postcolonial socio-legal scholarship sceptical of imported regulatory templates (Baxi 2008; Bhatia 2019).

4 The empirical horizon: who is the Indian data principal?

4.1 Digital literacy and the language question

The most recent Telecom Regulatory Authority of India figures place rural internet penetration in the vicinity of fifty percent, with a substantial portion of those users accessing the network through inexpensive smartphones whose interfaces are configured by default in English (Telecom Regulatory Authority of India 2024). The National Statistical Office's Comprehensive Annual Modular Survey (2022-23) found that only twenty-five percent of rural households had any member capable of operating a smartphone to perform tasks such as sending an email or filling an online form, compared with fifty-six percent in urban households (NSO 2024). Survey work on actual comprehension, as distinct from access, is even more sobering. The Policy Circle survey of 2025 reported that approximately thirty-eight percent of rural and semi-urban users said they meaningfully understood the digital products they used; a substantially larger fraction admitted that they clicked accept without reading, that they did not know what data they were agreeing to share, and that they had no clear recourse in the event of dispute (Policy Circle 2025).

The language dimension compounds the literacy dimension. The DPDP Act, in section 5(3) read with the 2025 Rules, requires notices to be made available in any language listed in the Eighth Schedule of the Constitution at the data principal's option. The provision is laudable in aspiration. In implementation, it places the burden of language selection on the user, who must navigate to it through interfaces that are usually defaulted to English. There is no parallel obligation on the Consent Manager to design its dashboard, withdrawal flows, grievance interfaces, or notification mechanisms in all twenty-two languages, nor to ensure that the substantive content of consent, as distinct from a translated label, is intelligible to a speaker of, say, Santhali, Maithili, or Konkani. The result is a regime that is formally multilingual and operationally monolingual.

4.2 Lessons from the Account Aggregator framework

The Account Aggregator (AA) framework, operationalised by the Reserve Bank of India in September 2021, is the closest analogue to the Consent Manager and is often cited as evidence that the model works in the Indian context. The growth statistics are striking. By February 2023, linked accounts crossed four million; by 2024, several major banks and non-banking financial companies had integrated AA-based consent flows; the Sahamati industry body reports exponential growth in successful consents (Sahamati 2024; Reserve Bank of India 2023).

Closer examination, however, reveals that the AA experience is consistent with rather than contradicts the critique developed here. Research conducted by the Consultative Group to Assist the Poor (CGAP) found that the principal driver of AA adoption was convenience in loan processing, that user awareness of the consent-based architecture remained low even among those who had used it, and that trust in the lender rather than understanding of the framework was the operative variable in user behaviour (CGAP 2025). A multi-sectoral study published in late 2025 found similar patterns: AA-mediated lending had reached significant volumes in micro-enterprise finance, but the empirical evidence on whether borrowers comprehended the data flows or experienced enhanced control was limited and often counter-intuitive (Advances in Consumer Research 2025). What the AA experience demonstrates is that a consent-intermediary architecture can be efficient at moving data; it does not demonstrate that it makes consent meaningful.

4.3 Dark patterns and the design of default

The Central Consumer Protection Authority, in its Guidelines for Prevention and Regulation of Dark Patterns of November 2023, identified thirteen specific dark-pattern practices, including drip pricing, basket sneaking, false urgency, confirm shaming, and disguised advertisements (Central Consumer Protection Authority 2023). The Guidelines are sectoral and limited in scope; the DPDP Act does not, on present reading, integrate them into the data-protection regime, nor do the 2025 Rules impose any specific obligation on Consent Managers to refrain from dark-pattern design. The Indian Council for Research on International Economic Relations (ICRIER) study of dark patterns in Indian e-commerce found that nearly seventy percent of leading apps deployed at least one dark-pattern element in their consent flows, with confirm-shaming and pre-checked consent boxes among the most prevalent (ICRIER 2023). Without an explicit duty on Consent Managers to design against such patterns, the architectural innovation of the dashboard risks being undone by the experiential reality of how that dashboard is presented to the user.

4.4 Children, women, and the household as data unit

Two further empirical features merit attention. The first is the situation of children. Section 9 of the DPDP Act and Rule 10 of the 2025 Rules impose a uniform requirement of verifiable parental consent for the processing of personal data of any person under eighteen years of age. The Consent Manager framework, in its present form, makes no provision for differentiated children's interfaces, nor does it address the well-documented problem that adolescents routinely circumvent age-gates and that the parental consent mechanism, mediated through DigiLocker, reintroduces precisely the aadhaar-anchored verification that Puttaswamy II treated with constitutional suspicion (Puttaswamy II, paragraphs 244-248).

The second is the situation of women in patriarchal households. Empirical work on intra-household digital access in India consistently finds that smartphones, when shared at all, are often controlled by men; that women's digital trails are routinely linked to accounts not in their own names; and that consent given through a single device cannot in any meaningful sense be attributed to a single individual (Sambasivan and others 2018; Donner 2015). A Consent Manager architecture that defaults to a one-device-one-person model is, in such settings, not protective but obscuring.

5 The constitutional dimension: equality, dignity, and proportionality

5.1 The proportionality test after Puttaswamy

The Supreme Court's elaboration of the right to informational privacy in Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1 set out a four-fold proportionality test: any infringement of the right must pursue a legitimate State aim, must bear a rational nexus to that aim, must be necessary in the sense that no less restrictive alternative is available, and must be proportionate stricto sensu, in the sense that the measure's benefits outweigh its costs (Puttaswamy, paragraphs 310-325 of Chandrachud J.). The proportionality test was reaffirmed and refined in Anuradha Bhasin v. Union of India (2020) 3 SCC 637 in the context of internet shutdowns, where the Court emphasised that the State must adopt the least restrictive means among those reasonably available.

Although Puttaswamy was concerned with State action, the proportionality framework has since been extended to evaluate the design of statutes that regulate private data processing. The DPDP Act is itself an expression of the State's obligation to give effect to the right; its institutional choices are therefore reviewable on the same standard. A Consent Manager design that imposes high entry barriers, defaults to English, ignores intra-household power dynamics, fails to address dark patterns, and presumes a uniform data principal across radically heterogeneous social settings does not obviously satisfy the necessity prong. Less restrictive alternatives, including obligatory linguistic accessibility standards, tiered registration regimes that admit non-commercial entities, and substantive design duties enforceable by the Board, exist and have been recognised in comparable jurisdictions.

5.2 Article 14 and indirect discrimination

The equality guarantee of Article 14 of the Constitution is concerned not only with formal classifications but, after Navtej Singh Johar v. Union of India (2018) 10 SCC 1 and Joseph Shine v. Union of India (2019) 3 SCC 39, with structures whose facially neutral design produces systematically unequal outcomes. The doctrine of indirect discrimination, expressly recognised by the Supreme Court in Lt. Col. Nitisha v. Union of India (2021) 15 SCC 125, requires the State to attend to the disparate impact of ostensibly general rules. A Consent Manager regime that is formally accessible to all but operationally accessible only to the digitally literate, the English-speaking, and the smartphone-equipped fails that doctrinal test. The remedy is not to abandon the architecture but to redesign it: to embed substantive accessibility duties into the registration conditions, to require differentiated interfaces for low-literacy users, and to subject Consent Managers to periodic accessibility audits commissioned by an entity independent of the Board's executive composition.

5.3 Article 21 and the right to be let alone

Puttaswamy located informational privacy at the intersection of Article 14, Article 19, and Article 21. Article 21's guarantee of life and personal liberty was read to include a right to autonomy, to dignity, and to be let alone (Puttaswamy, paragraphs 297-302 of Chandrachud J.). A consent regime that asks the data principal to make repeated, complex, granular decisions across a fragmented digital ecosystem is, in one sense, an instrument of autonomy; in another, it is the privatisation of a public obligation. The duty to design data systems that respect privacy by default and by design, articulated in section 25 of the General Data Protection Regulation and gestured at, but not operationalised, in the DPDP Act, is the appropriate constitutional response. To leave the burden on the data principal, mediated by an intermediary whose business model depends on the volume of consents flowing through its pipes, is to transfer to private actors a function that Article 21 places on the State.

6 Reform: from the algorithm shaping society to society shaping the algorithm

If the diagnosis offered above is broadly correct, the question becomes what is to be done. Five reform proposals follow. None requires legislative amendment in the first instance; each can be operationalised through delegated legislation, subordinate guidelines, or, in some cases, the Board's exercise of its certification and supervisory functions under Rule 4.

First, differentiated interface obligations. The Board's certification of a Consent Manager's interoperable platform under Rule 4(2)(e) should be conditioned on the demonstration of distinct interface modes for low-literacy users. The Reserve Bank of India's experience with the Account Aggregator framework offers a model: simplified, icon-led flows with audio support and intermediated literacy assistance are technically feasible and have been piloted in micro-finance settings (Sahamati 2024). A Consent Manager unable to demonstrate such modes ought not to be registered.

Second, mandatory linguistic accessibility. Rule 4 should be supplemented by a guideline requiring registered Consent Managers to provide their dashboards, notice interfaces, withdrawal flows, and grievance mechanisms in all twenty-two languages of the Eighth Schedule within a phased timeframe. The cost of such an obligation is real but bounded, and the constitutional case for it, after Puttaswamy and the indirect-discrimination doctrine of Nitisha, is strong.

Third, an independent grievance ombudsman. The ninety-day response timeline prescribed by the First Schedule is too long for many of the harms that the framework is meant to address, and it places resolution of disputes in the hands of the very intermediary against whom the grievance has been raised. An independent ombudsman, modelled on the Banking Ombudsman scheme of the Reserve Bank of India, would correct both deficiencies. Its decisions should be binding on the Consent Manager and subject to judicial review only on questions of law.

Fourth, an explicit prohibition on dark patterns. The Central Consumer Protection Authority's Guidelines of 2023 should be expressly incorporated into the registration conditions for Consent Managers. The Board's certification process should include a design audit, and the Board's annual report should publish aggregate findings on the prevalence of dark-pattern practices in registered Consent Managers' interfaces. Substantive design duties of this kind shift the regulatory centre of gravity from procedural compliance to outcome-oriented protection.

Fifth, a re-orientation of the regulator. The Data Protection Board of India is, on its present composition under sections 18 to 27 of the DPDP Act, an executive body. Its independence from the political branches is not statutorily secured to the degree that the Supreme Court has, in its tribunalisation jurisprudence beginning with L. Chandra Kumar v. Union of India (1997) 3 SCC 261 and continuing through Madras Bar Association v. Union of India (2021) 7 SCC 369, identified as constitutionally necessary. The Board's substantive mandate should be enlarged to include accessibility audits of Consent Managers, periodic public reporting on the demographics of consent flows, and consultation with civil-society representatives, including organisations working with women, children, persons with disabilities, and linguistic minorities. The journal's editorial commitment to society shaping the algorithm cannot be operationalised without an institution capable of carrying it forward.

7 Conclusion

The Consent Manager is, at its best, a serious attempt to address a serious problem. The fragmentation of digital consent, the cognitive impossibility of meaningful individual privacy self-management, the asymmetry between users and platforms, and the absence of mechanisms by which consent decisions can be reviewed, modified, and revoked are problems that have eluded most data-protection regimes in most jurisdictions. India has, in the DEPA and Account Aggregator lineage, contributed a distinctive institutional response. The recognition of the Consent Manager in the DPDP Act, and the operational architecture set out in the 2025 Rules, deserve careful and sympathetic engagement.

Sympathetic engagement, however, must not become uncritical adoption. The architecture as it stands embeds assumptions about the data principal that the Indian empirical record does not support, and it does so in a way that risks producing precisely the kind of algorithmic governance that the journal's editorial vision asks us to resist. The data principal who emerges from the rules is literate, English-speaking, smartphone-owning, time-rich, financially included, and individually situated. The data principal who emerges from the survey data, from the field reports of micro-finance institutions, from the work of feminist scholars of intra-household digital access, and from the constitutional jurisprudence of indirect discrimination is a more textured figure. She speaks, in many cases, a language not listed on the dashboard. She shares her device. She does not distinguish, with confidence, between a Consent Manager and a data fiduciary. She is the citizen-subject for whom the architecture must work, or it works for no one.

The reforms proposed in section 6 are modest in form and ambitious in aim. They ask the Board, the intermediaries, and the regulated community to undertake a re-design that places the empirical user, in her social, linguistic, and cognitive particularity, at the centre of the framework. They do not require legislative amendment; they require institutional resolve. Whether that resolve is forthcoming will determine whether the Indian Consent Manager becomes an instance of society shaping the algorithm, or another iteration of an algorithm shaping society from above. The answer to that question is not yet settled. It is, however, urgent.

Declarations

Funding The author received no specific funding for this work.

Conflicts of interest The author has no relevant financial or non-financial interests to disclose.

Ethical approval Not applicable. The article is doctrinal and theoretical and does not involve primary data collection from human subjects.

Data availability All sources cited are publicly available; no original datasets were generated.

Use of AI tools The author used a large-language-model assistant for AI-assisted copy editing within the meaning of Springer Nature's policy, namely improvements to grammar, style, and clarity of human-authored text. No substantive content, argument, or citation was generated by the model in a manner that would constitute authorship. All claims, citations, and analytical positions are the author's own and have been independently verified.

References

Advances in Consumer Research (2025) The transformative impact of the Account Aggregator framework on financial inclusion in India: a multi-sectoral study of MSMEs, microfinance, and personal lending. Adv Consum Res. https://acr-journal.com/article/the-transformative-impact-of-the-account-aggregator-framework-on-financial-inclusion-in-india-1852/

AZB & Partners (2026) Consent Managers under India's DPDP Act and DPDP Rules. AZB Insights, January 2026. https://www.azbpartners.com/bank/consent-managers-under-indias-dpdp-act-and-dpdp-rules/

Baxi U (2008) The future of human rights, 3rd edn. Oxford University Press, New Delhi

Bass, Berry & Sims (2026) India's data privacy rules: what your business needs to know. Bass Berry Sims PLC, 13 January 2026

Bhatia G (2019) The transformative constitution: a radical biography in nine acts. HarperCollins, Gurgaon

Central Consumer Protection Authority (2023) Guidelines for prevention and regulation of dark patterns. Ministry of Consumer Affairs, Food and Public Distribution, Government of India, 30 November 2023

Consultative Group to Assist the Poor (CGAP) (2025) Convenience drives rapid adoption of Account Aggregators in India. CGAP Blog, 1 April 2025. https://www.cgap.org/blog/convenience-drives-rapid-adoption-of-account-aggregators-in-india

Donner J (2015) After access: inclusion, development, and a more mobile internet. MIT Press, Cambridge MA

Government of India (2018) A free and fair digital economy: protecting privacy, empowering Indians. Report of the Committee of Experts under the chairmanship of Justice B.N. Srikrishna. Ministry of Electronics and Information Technology, New Delhi

Gunkel D J (2023) Editorial: from algorithmic governance to algorithmic accountability. AI & Soc 38(4):1431-1434

Indian Council for Research on International Economic Relations (ICRIER) (2023) Dark patterns in Indian e-commerce: an empirical study. ICRIER Working Paper Series, New Delhi

Lehtiniemi T, Kortesniemi Y (2017) Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. Big Data Soc 4(2):1-11. https://doi.org/10.1177/2053951717721935

Lexology (2025) Digital Personal Data Protection Rules, 2025: operationalising consent, security, and governance obligations. Lexology, 1 December 2025

McDonald A M, Cranor L F (2008) The cost of reading privacy policies. I/S J Law Policy Inf Soc 4(3):540-565

MediaNama (2025) Explained: role of Consent Managers as per DPDP Rules, 2025. MediaNama, 14 November 2025. https://www.medianama.com/2025/11/223-explained-obligations-role-requirements-consent-managers-dpdp-rules-2025/

Mejias U A, Couldry N (2019) Datafication. Internet Policy Rev 8(4). https://doi.org/10.14763/2019.4.1428

Mejias U A, Couldry N (2024) Data grab: the new colonialism of big tech and how to fight back. WH Allen, London

Ministry of Electronics and Information Technology (MeitY) (2022) Data Empowerment and Protection Architecture: draft for discussion. NITI Aayog, New Delhi

Ministry of Electronics and Information Technology (MeitY) (2025) Digital Personal Data Protection Rules, 2025. Gazette of India, Extraordinary, Part II, Section 3, Sub-section (i), 14 November 2025

National Statistical Office (2024) Comprehensive Annual Modular Survey (CAMS) 2022-23: report. Ministry of Statistics and Programme Implementation, Government of India

Nissenbaum H (2010) Privacy in context: technology, policy, and the integrity of social life. Stanford University Press, Stanford

Nissenbaum H (2011) A contextual approach to privacy online. Daedalus 140(4):32-48

Policy Circle (2025) Financial inclusion needs more than digital adoption. Policy Circle, 23 October 2025. https://www.policycircle.org/policy/financial-inclusion-digital-adoption/

Reserve Bank of India (2016) Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016. RBI/DNBR/2016-17/46, 2 September 2016

Reserve Bank of India (2023) Annual Report 2022-23. Reserve Bank of India, Mumbai

Sahamati (2023) Account Aggregator ecosystem: architecture and adoption. Sahamati Collective, Bengaluru

Sahamati (2024) State of the Account Aggregator ecosystem: 2024 annual report. Sahamati Collective, Bengaluru

Sambasivan N, Checkley G, Batool A, Ahmed N, Nemer D, Gaytan-Lugo L S, Matthews T, Consolvo S, Churchill E (2018) Privacy is not for me, it's for those rich women: performative privacy practices on mobile phones by women in South Asia. In: Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), USENIX Association, Baltimore MD, pp 127-142

Solove D J (2013) Privacy self-management and the consent dilemma. Harv Law Rev 126(7):1880-1903

Solove D J (2024) Murky consent: an approach to the fictions of consent in privacy law. Boston Univ Law Rev 104(2):593-639

Telecom Regulatory Authority of India (2024) The Indian telecom services performance indicators: January-March 2024. TRAI, New Delhi

Tsaaro (2025) Consent Managers under the DPDP Act and DPDP Rules, 2025: functions, obligations, and governance. Tsaaro Privacy Insights, November 2025. https://tsaaro.com/blogs/consent-managers-under-the-dpdp-act-and-dpdp-rules-2025

Zuboff S (2019) The age of surveillance capitalism: the fight for a human future at the new frontier of power. PublicAffairs, New York

Cases

Anuradha Bhasin v. Union of India (2020) 3 SCC 637 (Supreme Court of India)

Joseph Shine v. Union of India (2019) 3 SCC 39 (Supreme Court of India)

Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (Supreme Court of India, Nine-Judge Bench)

Justice K.S. Puttaswamy (Retd.) v. Union of India (2019) 1 SCC 1 (Aadhaar judgment, Five-Judge Bench, hereafter Puttaswamy II)

L. Chandra Kumar v. Union of India (1997) 3 SCC 261 (Supreme Court of India)

Lt. Col. Nitisha v. Union of India (2021) 15 SCC 125 (Supreme Court of India)

Madras Bar Association v. Union of India (2021) 7 SCC 369 (Supreme Court of India)

Navtej Singh Johar v. Union of India (2018) 10 SCC 1 (Supreme Court of India)

Statutes and rules

Constitution of India, 1950

Digital Personal Data Protection Act, 2023 (Act 22 of 2023)

Digital Personal Data Protection Rules, 2025, Gazette of India, 14 November 2025

Personal Data Protection Bill, 2019 (Bill No. 373 of 2019)