SHADOW PROFILES AND THE RIGHT TO BE FORGOTTEN: A GAP IN INDIA'S DPDPA

Daksh Verma, Law College Dehradun, Uttaranchal University

Prof. (Dr.) Anil Kumar Dixit, Law College Dehradun, Uttaranchal University

ABSTRACT

The Digital Personal Data Protection Act, 2023 marks a watershed moment in India's privacy jurisprudence, operationalising the constitutional guarantee articulated in Justice K.S. Puttaswamy v. Union of India through a consent-centric architecture. Yet the Act's reliance on a binary relationship between the "data principal" and the "data fiduciary," combined with its restrictive definition of personal data, leaves a structural lacuna: the phenomenon of shadow profiles. Shadow profiles—dossiers algorithmically constructed from inferred attributes, contact harvesting, device fingerprinting, and third-party disclosures concerning individuals who have never registered with or consented to a particular data fiduciary—exist at the periphery of the DPDPA's protective ambit. This article contends that the right to erasure under Section 12 cannot reach these profiles because (a) the statute presumes a consensual touchpoint between data principal and data fiduciary; (b) inferred and derived data, which constitutes the very fabric of shadow profiles, finds no explicit recognition; and (c) non-users—the principal subjects of shadow profiles—lack effective standing under the Act. By contrasting the DPDPA's approach with Article 17 of the General Data Protection Regulation and the European Court of Justice's jurisprudence beginning with Google Spain v. AEPD, this article demonstrates that India's right to be forgotten is most deficient where it is most necessary. Drawing on the proportionality test in Puttaswamy, the article advances four reforms: explicit statutory recognition of inferred data; a disclosure-and-erasure right for non-users; mandatory shadow-profile auditing for Significant Data Fiduciaries; and a proactive notification mandate. Absent these interventions, the right to be forgotten in India risks becoming an entitlement only the already-visible may invoke.

Keywords: Shadow Profiles, Right to Be Forgotten, DPDPA, Inferred Data, Informational Privacy, Puttaswamy, GDPR, Significant Data Fiduciary.

I. INTRODUCTION

The architecture of contemporary digital surveillance does not rest on the visible interaction between user and platform alone. Beneath the consent-laden surface of every login screen and privacy notice lies a parallel data infrastructure—one populated by individuals who have never enrolled, never visited, and often never even heard of the entity collecting information about them. The data scientist Aleksandr Kogan, in evidence before the United Kingdom Parliament, conceded that platforms routinely build "shadow profiles" of non-users by aggregating information harvested from registered users.[1] In 2018, journalists revealed that Facebook used contact-list synchronisation, browser cookies, and device identifiers to construct dossiers on individuals who had not signed up for the service, leveraging this latent population of non-users to predict relationships, infer interests, and tailor advertising.[2] Such revelations triggered regulatory inquiries in Europe but have, until recently, occupied the legislative periphery in India.

The Digital Personal Data Protection Act, 2023[3] (the "DPDPA") was enacted as the culmination of nearly six years of debate following the Supreme Court's recognition of informational privacy as a facet of Article 21 in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[4] The statute is, in many respects, an act of consolidation: it codifies obligations that fiduciaries already faced in the abstract under *Puttaswamy* and brings India broadly within the global mainstream of data-protection regimes. Yet the DPDPA, as ultimately enacted, is also an act of textual minimalism. It is shorter than the Personal Data Protection Bill, 2019 it replaced; it omits express recognition of categories such as sensitive personal data; and, most significantly for present purposes, it contemplates the data-principal/data-fiduciary relationship as a discrete, voluntary one, initiated by the principal's consent or by another lawful ground enumerated in Section 7.

This article identifies a doctrinal and definitional gap within the DPDPA: the right to erasure under Section 12 cannot, by its plain text, reach shadow profiles. The argument unfolds in seven Parts. Part II describes the technological architecture of shadow profiles and the

[1]Damian Collins, MP, Chair, House of Commons Digital, Culture, Media & Sport Comm., Letter to Mike Schroepfer, Chief Tech. Officer, Facebook (May 14, 2018) (acknowledging the construction of profiles based on data drawn from non-users).
[2]Nitasha Tiku, Facebook's 'Shadow Profiles' Are the Stuff of Nightmares, Wired (June 28, 2018), https://www.wired.com.
[3]Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India) [hereinafter DPDPA].
[4]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) [hereinafter Puttaswamy].

typology of inferred data on which they depend. Part III traces the conceptual lineage of the right to be forgotten from European Court of Justice jurisprudence to its constitutional anchoring in *Puttaswamy*. Part IV analyses the DPDPA's text and demonstrates that its key concepts—data principal, personal data, processing—are calibrated to a registration-based model of data acquisition that does not accommodate the non-consensual aggregation characteristic of shadow profiles. Part V undertakes a comparative analysis with the General Data Protection Regulation,[5] showing that even the GDPR's relatively expansive Article 17 has struggled with shadow-profile cases, and that the DPDPA's narrower text is consequently more vulnerable. Part VI articulates a constitutional critique grounded in the proportionality framework of *Puttaswamy*. Part VII offers four concrete reform proposals, and Part VIII concludes.

The thesis is straightforward. Without targeted statutory amendment or robust subordinate regulation under Section 40, the DPDPA will codify an unequal privacy regime in which only those individuals who voluntarily transact with a data fiduciary are protected, while those most vulnerable to invisible aggregation are left outside the Act's remedies. The right to be forgotten cannot mean a right available only to those whom the digital economy has already remembered.

II. WHAT IS A SHADOW PROFILE?

A. Definitional Core

A "shadow profile" denotes a dataset compiled by a data processor about a natural person who has not created an account, has not registered, and may not even be aware of the data processor's existence. The term acquired public salience in 2013 when a Facebook security flaw revealed that the platform held aggregated contact information for individuals who had never signed up.[6] Shadow profiles are not anomalous artefacts of any single platform; they are systemic outputs of three interlocking practices common to digital infrastructure: contact-list ingestion, cross-site identification through cookies and pixels, and predictive modelling of relationships and attributes from observed user behaviour.[7]

[5]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
[6]Kashmir Hill, Facebook's Shadow Profiles: 'Friend Suggestions' from People You Haven't Met, Forbes (June 26, 2013), https://www.forbes.com.
[7]Solon Barocas & Helen Nissenbaum, Big Data's End Run Around Anonymity and Consent, in Privacy, Big Data,

The shadow profile differs from traditional categories recognised in privacy law in two structural respects. First, the data subject has not contracted, consented, or even interacted with the controller. Second, much of the information aggregated in such a profile is not directly observed but inferred—generated by statistical models that estimate, for example, the email address, location, age, employer, or social affiliations of the individual.[8] These two attributes together place shadow profiles outside the conventional grid of "collected" and "disclosed" personal data on which most data-protection statutes, including the DPDPA, are constructed.

B. Mechanisms of Construction

Shadow profiles emerge from at least five distinct technical mechanisms. The first is *contact harvesting*: when an existing user permits a service to access her phone book, the service ingests not only her own data but the names, phone numbers, and email addresses of every contact in her device—each of whom is now indexed in the controller's database without notice or consent.[9] The second is *web-tracking infrastructure*: third-party cookies, embedded pixels, and software development kits installed in popular applications report visit-level data back to controllers, who assign persistent identifiers to non-user browsers.[10] The third is *data brokering*: controllers purchase or licence datasets from data brokers, who in turn assemble information from public records, loyalty programmes, voter rolls, and other sources, and sell it as enrichment for existing customer files.[11] The fourth is *inference*: machine-learning models predict missing attributes about an individual from associated data, such that even where direct collection is absent, an attribute may be assigned with high confidence.[12] The fifth is *graph aggregation*: relational databases connect identifiers across these sources, allowing a controller to assemble a single, coherent profile of a non-user by stitching fragmentary observations together.

Each mechanism presents distinct legal challenges. Contact harvesting raises questions of indirect collection. Web-tracking raises questions about the scope of personal data. Data brokering raises questions about the legality of acquisition without lawful basis. Inference

---

and the Public Good 44, 47–50 (Julia Lane et al. eds., 2014).

[8]Sandra Wachter & Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, 2019 Colum. Bus. L. Rev. 494, 511–15.

[9]See Jennifer Valentino-DeVries et al., How Apps Track You Even When You Tell Them Not To, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com.

[10]Joel R. Reidenberg et al., Privacy Harms and the Effectiveness of the Notice and Choice Framework, 11 I/S: J.L. & Pol'y for Info. Soc'y 485, 506–09 (2015).

[11]Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability 11–15 (2014).

[12]Wachter & Mittelstadt, supra note 8, at 530.

raises questions about whether predicted attributes count as personal data at all. Graph aggregation raises questions about the data principal's identity in a context where no single data point is principal-supplied. The DPDPA's silence across these dimensions is the central concern of this article.

C. The Indian Context

India has not been spared shadow-profile practices. The Telecom Regulatory Authority of India has reported that contact-harvesting through SDKs embedded in applications hosted on Indian app stores is widespread.[13] In 2021, an investigation revealed that several large advertising-technology platforms operating in India built behavioural dossiers on Indian internet users by tracking visits across more than fourteen thousand websites, including for users who had not registered with any of the underlying platforms.[14] More recently, the Indian Computer Emergency Response Team (CERT-In) issued advisories noting that aggregated datasets allegedly compiled from Indian users had appeared on dark-web marketplaces, with portions of those datasets corresponding to individuals who had never directly transacted with the data fiduciary alleged to be the source.[15] The Indian context is therefore not theoretical; it is an active site of shadow-profile activity demanding regulatory attention.

III. THE RIGHT TO BE FORGOTTEN: A BRIEF GENEALOGY

A. European Origins

The right to be forgotten ("RTBF") emerged from European data-protection law as a doctrinal response to the persistence of digital information. In 2014, the Court of Justice of the European Union in *Google Spain SL v. Agencia Española de Protección de Datos*[16] held that an individual could compel a search-engine operator to de-list links to lawfully published information that had become "inadequate, irrelevant or no longer relevant" to the original purpose of processing. The decision rested on Articles 12(b) and 14(a) of the then-extant Data Protection Directive 95/46/EC and inaugurated a sustained jurisprudential evolution.

[13]Telecom Regulatory Auth. of India, Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector 24–26 (July 16, 2018).
[14]The Reporters' Collective, How Online Trackers Map the Indian Internet, The Wire (Aug. 12, 2021), https://thewire.in.
[15]Indian Computer Emergency Response Team (CERT-In), Vulnerability Note CIVN-2023-0287 (Nov. 14, 2023).
[16]Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶¶ 92–94 [hereinafter Google Spain].

The General Data Protection Regulation, in force since 2018, codified and extended this principle in Article 17. The right to erasure under Article 17 obliges a controller to erase personal data "without undue delay" where, *inter alia*, the data are no longer necessary, the data subject withdraws consent, the data subject objects, the data have been unlawfully processed, or erasure is required by law.[17] Critically for the present analysis, Article 17(2) extends the obligation to controllers who have made the data public, requiring them to take reasonable steps—including technical measures—to inform other controllers processing the data of the erasure request.[18] This dissemination-cascade rule is precisely the textual feature that the DPDPA omits.

B. Constitutional Recognition in India

In India, the conceptual antecedents of RTBF were judicially developed before any data-protection statute was enacted. The Karnataka High Court in *Sri Vasunathan v. Registrar General*[19] permitted the redaction of a woman's name from publicly available judgments concerning matrimonial disputes; the Delhi High Court in *Jorawer Singh Mundy v. Union of India*[20] directed the de-indexing of a judgment from search engines after the petitioner had been acquitted of charges. These decisions, though factually narrow, signalled judicial willingness to read RTBF into Article 21's privacy guarantee.

The Supreme Court's nine-judge decision in *Puttaswamy*[21] cemented the constitutional foundation. Justice S.K. Kaul's concurring opinion observed that "the right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the internet."[22] Justice Kaul went further to recognise the right to be forgotten as a facet of informational privacy, although he tempered its application with limitations relating to public interest, freedom of expression, and the historical record. The decision did not enact RTBF; it created the constitutional space within which legislation could.

[17]GDPR, supra note 5, art. 17(1).
[18]Id. art. 17(2); see also id. recital 66.
[19]Sri Vasunathan v. Registrar General, 2017 SCC OnLine Kar 424 (India).
[20]Jorawer Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306 (India).
[21]Puttaswamy, supra note 4.
[22]Id. ¶ 638 (Kaul, J., concurring) (recognising the right to control one's existence on the internet as part of informational privacy).

C. RTBF in the DPDPA

The DPDPA gives statutory form to RTBF in Section 12, which empowers the data principal to seek "erasure of her personal data," subject to retention required by law.[23] Section 8(7) imposes a corresponding obligation on the data fiduciary to erase personal data upon withdrawal of consent or upon the conclusion of the specified purpose.[24] These two provisions, read together, constitute the DPDPA's RTBF architecture. As examined in the next Part, however, this architecture rests on assumptions that the shadow-profile phenomenon decisively disproves.

IV. THE STRUCTURAL GAP: WHY THE DPDPA CANNOT REACH SHADOW PROFILES

A. The Definition of "Data Principal"

Section 2(i) of the DPDPA defines the data principal as "the individual to whom the personal data relates."[25] On its face, this definition is broad enough to include non-users: where data relates to an individual, that individual is the data principal regardless of whether she has consented to processing. Yet the operational provisions of the Act—particularly Section 5 (notice), Section 6 (consent), Section 7 (legitimate uses), and Section 11 (right to access)—presuppose that the data principal can be identified by the data fiduciary and addressed through a notice mechanism. For shadow profiles, the data fiduciary may not have contact information for the data principal at all; the very absence of such direct identifiers is what marks the data subject as a non-user.

This produces a doctrinal asymmetry. The data principal exists, in theory, the moment data "relates" to her. But she cannot exercise her rights, because she does not know that she is a principal, and she cannot easily learn of the existence of a profile, because the DPDPA imposes no proactive notification obligation on data fiduciaries vis-à-vis non-users. The right is real; it is only inaccessible.

B. The Definition of "Personal Data"

Section 2(t) defines personal data as "any data about an individual who is identifiable

[23]DPDPA, supra note 3, Sec. 12(1)–(3).
[24]Id. Sec. 8(7).
[25]Id. Sec. 2(i) (defining "Data Principal" as "the individual to whom the personal data relates").

by or in relation to such data."[26] Whether inferred attributes—predicted age, predicted location, predicted relationship status—qualify as personal data turns on the meaning of "about." European jurisprudence has treated inferred data as personal data when the inference is used to make decisions affecting the individual.[27] The DPDPA's text is silent on inferred data, and the Government has not yet promulgated rules under Section 40 that would clarify the position.

The silence is consequential. If inferred data falls outside personal data, then the entire predictive layer that animates shadow profiles is unregulated. If it falls within personal data, then questions of data minimisation and accuracy attach. The textual ambiguity creates an enforcement vacuum. Indian courts will likely be required to construe Section 2(t) purposively, but absent express provision, data fiduciaries can advance plausible textual readings that exclude inferred outputs from regulatory scrutiny.

C. Consent and the Lawful-Basis Architecture

Section 4(1) provides that personal data may be processed "only in accordance with the provisions of this Act."[28] Section 4(1)(a) requires either consent under Section 6 or a "legitimate use" listed in Section 7. Shadow profiles are constructed without consent, by definition. The question is whether any legitimate use accommodates them.

Section 7 enumerates eight legitimate uses, including voluntary provision by the data principal, performance of state functions, compliance with judgments, medical emergencies, employment, and certain public-interest activities.[29] None plausibly authorises the construction of a shadow profile of a non-user for commercial purposes. The Act conspicuously omits a "legitimate interests" basis comparable to Article 6(1)(f) of the GDPR.[30] This omission cuts both ways. On one hand, it removes the most likely basis on which data fiduciaries might justify shadow-profile construction. On the other, it leaves shadow profiles—if they exist—in a regulatory limbo: they are constructed without lawful basis and are therefore unlawful, but the Act provides no specific remedy for the data principal who is unaware of their existence.

[26]Id. Sec. 2(t) (defining "personal data").
[27]Case C-434/16, Nowak v. Data Prot. Comm'r, ECLI:EU:C:2017:994, ¶¶ 34–35.
[28]DPDPA, supra note 3, Sec. 4(1).
[29]Id. Sec. 7.
[30]GDPR, supra note 5, art. 6(1)(f).

D. Section 8 Obligations

Section 8 enumerates the obligations of a data fiduciary. Sub-section (3) requires the fiduciary to ensure the "completeness, accuracy and consistency" of personal data used to make decisions affecting the data principal or to disclose to another fiduciary.[31] Sub-section (4) requires reasonable security safeguards. Sub-section (5) requires breach notification. Sub-section (7) prescribes the period for which personal data may be retained. Critically, none of these provisions imposes a proactive disclosure obligation on data fiduciaries with respect to non-users. The Act presumes that the data principal will trigger the fiduciary's obligations through a request—but a non-user cannot make such a request without first knowing that her data is being processed.

E. Section 12: The Right to Correction and Erasure

Section 12(1) confers on the data principal "the right to correction, completion, updating and erasure of her personal data" for which she had previously given consent.[32] The text of Section 12 is the most consequential drafting decision for the present analysis. By tying the right of erasure to data "for which she had previously given consent," Section 12 textually excludes data processed without consent—including, on a strict reading, data in shadow profiles.

This is the core gap. A non-user cannot have given consent. If consent is the textual trigger for erasure, the non-user is excluded from Section 12. To the extent that shadow profiles are processed under one of the legitimate uses in Section 7—which, as noted, is unlikely on the present text—Section 12 would still require the data principal to have a transactional history with the fiduciary, a precondition that the shadow-profile context fundamentally negates.

There is a counter-argument: the right to erasure can be reconstructed from the unlawfulness of processing itself. If shadow profiles are processed without lawful basis, they violate Section 4(1) and ought to be erased as a matter of statutory compliance rather than as the exercise of a Section 12 right. This counter-argument is theoretically sound but practically inert. Without a complaint mechanism accessible to non-users, the unlawfulness of shadow profiles will go undetected. The Data Protection Board of India, constituted under Section 18,

[31]DPDPA, supra note 3, Sec. 8(3).
[32]Id. Sec. 12(1).

can act on its own motion or on referral, but the absence of disclosure obligations means that the Board's information base will systematically under-represent shadow profiles.[33]

F. Significant Data Fiduciaries

Section 10 empowers the Central Government to designate Significant Data Fiduciaries ("SDFs") on the basis of factors including the volume and sensitivity of data processed.[34] SDFs are subject to enhanced obligations including the appointment of a Data Protection Officer, periodic data-protection impact assessments, and audits. The SDF designation is the most plausible route within the existing Act for addressing shadow profiles, because the largest aggregators of non-user data will almost certainly fall within the SDF category.

Yet Section 10's enhanced obligations do not specifically include shadow-profile mapping or non-user disclosure. A data-protection impact assessment under Section 10(2)(c) will identify risks attendant on a designated processing activity, but a fiduciary that does not classify shadow-profile aggregation as a discrete processing activity may simply omit it from the assessment. Without subordinate regulation that names shadow profiles as a defined risk, the DPIA mechanism will not surface the issue.

V. COMPARATIVE ANALYSIS: GDPR AS A REFERENCE POINT

The GDPR is the natural comparator for the DPDPA, but the comparison reveals a paradox. The GDPR is itself imperfectly equipped to regulate shadow profiles, and yet the DPDPA's architecture is significantly weaker on multiple metrics.

A. Definitional Scope

Article 4(1) of the GDPR defines personal data as "any information relating to an identified or identifiable natural person."[35] The European Data Protection Board has clarified, in successive guidelines, that inferred and derived data fall within this scope.[36] The DPDPA's phrasing—"any data about an individual who is identifiable by or in relation to such data"—is in some respects narrower, both because "data about" suggests a directness of attribution and

[33]See id. Secs. 18–27 (constitution and powers of the Data Protection Board of India).
[34]Id. Sec. 10(1).
[35]GDPR, supra note 5, art. 4(1).
[36]European Data Prot. Bd., Guidelines 4/2019 on Article 25 Data Protection by Design and by Default ¶¶ 73–76 (Oct. 20, 2020).

because the absence of regulatory guidance on inferred data leaves the question contested. A textual reading favourable to data fiduciaries could exclude many shadow-profile outputs from the definition altogether.

B. Lawful Basis

Article 6(1) of the GDPR enumerates six lawful bases for processing, including the legitimate-interest basis under Article 6(1)(f).[37] The Article 29 Working Party (now European Data Protection Board) explicitly considered shadow-profile construction in its Opinion 06/2014, concluding that the legitimate-interest basis cannot be invoked where the rights and freedoms of the data subject override the controller's interests.[38] In practice, this has prevented controllers from justifying shadow-profile construction under the legitimate-interest test. The DPDPA, by contrast, omits a legitimate-interest basis altogether, which makes shadow-profile construction unlawful in principle—but, as discussed, leaves the enforcement architecture inadequate.

C. Article 17 RTBF

Article 17 GDPR confers a right to erasure on broader grounds than DPDPA Section 12. It applies where data have been unlawfully processed, where the data subject objects under Article 21, where the data are no longer necessary, and in other circumstances. Article 17(2) further requires controllers who have made personal data public to inform other controllers of the erasure request. The DPDPA contains no analogue to Article 17(2)—a critical omission in the shadow-profile context, where the controller's information may be onward-shared through advertising networks and data brokers.

D. Right to Object

Article 21 GDPR confers a right to object to processing, including profiling, that does not depend on prior consent.[39] This right is the principal European doctrinal vehicle through which non-users might, in theory, contest shadow profiles. The DPDPA contains no equivalent right to object to non-consensual processing. Section 13 confers a right to grievance redressal

[37]GDPR, supra note 5, art. 6(1).
[38]Article 29 Data Prot. Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller, WP 217, at 30–32 (Apr. 9, 2014).
[39]GDPR, supra note 5, art. 21(1).

through the data fiduciary's own mechanism,[40] but this presumes that the data principal can identify the fiduciary in question. In the shadow-profile context, that presumption is precisely what fails.

E. Enforcement Architecture

The GDPR's enforcement is decentralised across national supervisory authorities, with a coordinating role for the European Data Protection Board.[41] The DPDPA centralises enforcement in the Data Protection Board of India. Sections 27 and 28 enable the Board to issue directions and impose penalties.[42] The Board's effectiveness will turn on the rules promulgated under Section 40 and the resources allocated to it. For the shadow-profile question, the Board will need both a clear statutory mandate to scrutinise non-user data and the technical capacity to audit complex aggregation systems.

VI. THE CONSTITUTIONAL DIMENSION

A. Puttaswamy and Informational Privacy

The conclusion that the DPDPA inadequately regulates shadow profiles is not merely a critique of statutory drafting; it raises constitutional questions. The Supreme Court in *Puttaswamy* held that informational privacy is a constituent of the right to life and personal liberty under Article 21, and that any state action restricting privacy must satisfy the proportionality test articulated in *Modern Dental College & Research Centre v. State of M.P.*[43] Although *Puttaswamy* concerned vertical state action, its rationale extends to horizontal arrangements operationalised through statute: where legislation purports to govern privacy, the resulting regime must itself be proportional to its objectives.

A regime that protects only consenting users from data aggregation, while leaving non-users without remedy, fails the proportionality test in three respects. First, it under-inclusively addresses a significant subset of privacy harms (shadow profiles) without articulating a constitutionally legitimate reason for the exclusion. Second, the means selected (consent-based architecture) are not necessary for the legitimate aim (privacy protection); a notice-and-erasure

[40]DPDPA, supra note 3, Sec. 13.
[41]GDPR, supra note 5, ch. VII (cooperation and consistency mechanism).
[42]DPDPA, supra note 3, Secs. 27–28.
[43]Modern Dental Coll. & Research Ctr. v. State of M.P., (2016) 7 SCC 353, ¶ 64 (India), adopted in Puttaswamy, (2017) 10 SCC 1, ¶ 310.

mechanism for non-users would be no more burdensome than the existing regime for users. Third, the asymmetric protection produces a disproportionate impact on those least able to control their digital exposure—precisely the population that the right to privacy was articulated to defend.

B. Equality Concerns

The DPDPA's architecture may also raise concerns under Article 14. By extending statutory protection only to those individuals who have entered the consent ecosystem, the Act creates an intelligible differentia between users and non-users. Whether that differentia bears a rational nexus to the object of the Act—comprehensive data protection—is contestable. The object of the Act, as recited in its preamble, is to "provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes."[44] The exclusion of non-users from substantive remedies cannot easily be reconciled with the object so framed.

C. Article 19 and the Right to Receive

A subsidiary concern relates to Article 19(1)(a). The right to receive information includes the right to know what information is held about oneself.[45] If the data fiduciary is under no obligation to disclose its possession of a shadow profile, the data principal's Article 19(1)(a) interest is functionally hollow. The DPDPA's right to access under Section 11 is again limited to "personal data being processed by such Data Fiduciary, pursuant to any consent given by the Data Principal,"[46] textually replicating the consent-trigger problem identified in relation to Section 12. The Act, in this respect, fails to operationalise the very informational interest that *Puttaswamy* was decided to protect.

VII. RECOMMENDATIONS

To close the shadow-profile gap, four reforms are necessary. They can be implemented through a combination of statutory amendment and subordinate regulation under Section 40 of the DPDPA.

[44]DPDPA, supra note 3, pmbl.
[45]Sec'y, Ministry of Info. & Broad. v. Cricket Ass'n of Bengal, (1995) 2 SCC 161, ¶ 75 (India).
[46]DPDPA, supra note 3, Sec. 11(1).

A. Express Recognition of Inferred Data

Section 2(t) should be amended, or rules should clarify, that personal data includes inferred, derived, and predicted data where such data is used to make decisions affecting the individual or is associated with an identifier capable of distinguishing the individual. This would align India with the European position articulated in *Nowak*[47] and resolve the central definitional ambiguity that allows shadow-profile architects to characterise their outputs as "non-personal." The amendment should further clarify that probabilistic inferences—such as predicted gender, predicted income bracket, or predicted political affiliation—are personal data when the controller acts upon them, regardless of whether the data principal would recognise them as accurate.

B. A Disclosure-and-Erasure Right for Non-Users

A new sub-section in Section 11 should grant any individual—whether or not she has previously consented to processing—the right to query a data fiduciary regarding the existence of personal data relating to her, and to demand erasure where such data has been processed without lawful basis. This right would be analogous to Article 15 GDPR's right of access,[48] broadened to non-consensual contexts. The right should be exercisable through a standardised online portal maintained by every data fiduciary above a notified threshold, with response timelines mirroring those in Section 5(2). To prevent abuse, the data fiduciary should be permitted to charge a nominal fee for repeat queries within short intervals, but never for the first query in a calendar year.

C. Mandatory Shadow-Profile Audits for SDFs

Subordinate regulation under Section 10 should require Significant Data Fiduciaries to conduct annual audits identifying all categories of personal data held about non-users, the lawful basis (if any) for such processing, and the volume and demographic distribution of such data. Audit reports should be filed with the Data Protection Board of India, and a redacted summary published. The audit obligation should be paired with a corresponding obligation to delete personal data of non-users for which no lawful basis can be identified, within a defined remediation period. This audit-and-delete mechanism is the structural counterpart to the

[47]Nowak, supra note 27.
[48]GDPR, supra note 5, art. 15.

individual erasure right and is necessary because individual rights cannot, on their own, surface the volume of latent processing characteristic of shadow profiles.

D. Proactive Notification Mandate

A new provision should require that, upon any onward use of non-user data—for instance, contact with an individual based on a shadow profile—the data fiduciary disclose the source and nature of the data in the same medium as the contact. This proactive obligation would trigger the cascade of substantive rights that, under the current text, depend on the principal's pre-existing knowledge. The notification should specify (i) the data fiduciary's identity, (ii) the categories of data held, (iii) the source of those data, and (iv) the data principal's rights under Sections 11–14 of the Act. The Central Government, in exercise of its rule-making power under Section 40,[49] is well-equipped to operationalise this mandate without legislative amendment, although a statutory anchor would be preferable.

These reforms would not eliminate shadow profiles. They would, however, equip the DPDPA to meet the challenges that shadow-profile architectures pose. They would also ground the DPDPA's promise—that India's privacy regime is one of the most protective in the world—on a foundation that does not reward concealment.

VIII. CONCLUSION

The DPDPA represents a foundational achievement in Indian privacy law. Yet the right to be forgotten that it inscribes is structurally calibrated to the visible: only those who have engaged a data fiduciary can demand erasure of what the fiduciary holds. The shadow-profile phenomenon, by contrast, depends on invisibility—on the absence of registration, consent, and direct interaction. To leave the right to be forgotten textually conditioned on consent is to leave the right unavailable precisely when it is most needed.

This is not a marginal infirmity. The economic logic of contemporary digital infrastructure increasingly depends on aggregated information about non-users; the Indian data ecosystem exhibits the same patterns observed elsewhere; and the constitutional vision in *Puttaswamy* admits no exception for the non-consenting. The DPDPA's architecture is repairable, but only if the legislature, or the Government acting through Section 40, recognises

[49]DPDPA, supra note 3, Sec. 40.

that a regime which limits privacy rights to those who have already entered the data economy underdelivers on its constitutional foundation. The reforms proposed in this article are calibrated to that recognition. Without them, the Indian "right to be forgotten" remains an entitlement of the visible—a doctrinal half-measure that cannot meet the technologies of invisible aggregation it was framed to address.

The legitimacy of a privacy statute is tested not by what it offers those it can see, but by whether it speaks for those it cannot. The DPDPA, as it stands, fails that test. Closing the shadow-profile gap is therefore not a question of regulatory housekeeping. It is a question of whether India's data-protection regime can deliver on the constitutional promise from which it draws its authority.