JOURNAL OF LAW, INFORMATION & SCIENCE
ISSN 0729-1485• Vol. 1, Issue 1 (2023) • https://jlisjournal.com/

REVIEW ARTICLE Article ID: JLIS/2023/1/1/007

Publication Without Obligation: Section 4 of the Right to Information Act, 2005, the Open Government Data Policy and the Limits of Proactive Disclosure in India

Zoha Khan[1], Dr. Jai Veer Singh [2]

[1] Research Scholar, Department of Law, Center of Advanced Legal Studies, Kamla Nehru College.
[2] Professor, Department of Law, Center of Advanced Legal Studies, Kamla Nehru College.

Received: 28 May 2023 **Revised:** 28 June 2023 **Accepted:** 11 September 2023 **Published:** 21 October 2023

ABSTRACT

Indian transparency law rests on two distinct mechanisms. The first is reactive: a citizen files a request and a public authority answers. The second is proactive: the authority publishes without being asked. Section 4 of the Right to Information Act, 2005 was drafted to make the second mechanism dominant, and expressly declares the objective of minimising resort to the request procedure. Two decades later, the reactive mechanism carries almost the entire burden of the statute, while the proactive mechanism has migrated without legislative authority and without justiciable entitlement into a layer of executive policy comprising the National Data Sharing and Accessibility Policy, 2012, the Open Government Data Platform, and the emerging national data governance framework. This article argues that the migration has produced an accountability deficit of a specific kind. Volume of published data has risen while explanatory transparency has fallen, because the datasets released are selected by the disclosing authority rather than demanded by the citizen, because no remedy attaches to non-release, and because the fastest-growing category of governmental decision-making automated and semi-automated determinations made within digital public infrastructure generates records that the open-data layer does not publish and that the reactive layer struggles to reach. Drawing on the distinction between technological openness and political accountability, and on the information-science literature on metadata quality and machine-readability, the article proposes that Section 4 be given enforceable content, that a statutory duty of algorithmic disclosure be recognised, and that India's open-data policy be placed on a legislative footing comparable to the European Open Data Directive and the United States OPEN Government Data Act.

Keywords: *Right to Information Act 2005; informational privacy; public interest override; transparency.*

1. Introduction

The Right to Information Act, 2005 is remembered as a statute about asking. Its popular iconography is the citizen at the counter, the ten-rupee application, the reluctant clerk. That iconography is accurate as a description of practice but inaccurate as a description of design. The Act was drafted on the assumption that requests would be exceptional and publication routine. Section 4(2) states the assumption explicitly: every public authority shall endeavour to provide as much information suo motu to the public at regular intervals so that the public have minimum resort to the use of the Act to obtain information.

That endeavour has not succeeded. The reason is not obscure. The Act attaches a penalty to the wrongful refusal of a request but attaches nothing at all to the failure to publish. An obligation without a sanction, addressed to an institution rather than to a named officer, and unaccompanied by any audit requirement in the parent statute, is a weak obligation. Over eighteen years it has weakened further as the practical work of publication has migrated to a parallel structure built on executive policy rather than statute: the National Data Sharing and Accessibility Policy, 2012, the Open Government Data Platform at data.gov.in, and, more recently, a national data governance framework oriented as much towards artificial intelligence development as towards public accountability.

This article makes three claims. First, that the proactive limb of Indian transparency law has been effectively de-legalised: the duty remains in the statute, but the activity now occurs under policy instruments that create no entitlement and no remedy. Second, that the resulting publication is systematically mismatched with accountability, because the disclosing authority selects what to disclose. Third, that this mismatch is becoming acute as governmental decisions are increasingly made within digital public infrastructure, where the operative record is not a file but a rule expressed in code. Parts 2 to 4 describe the two layers. Part 5 analyses the legal character of open data in India. Part 6 addresses algorithmic opacity. Part 7 sets out the information-science preconditions of useful disclosure. Part 8 draws comparative lessons.

2. The Architecture of Section 8(1)(j) Before 2023

The unamended Section 8(1)(j) exempted from disclosure "information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information". A proviso added that information which cannot be denied to Parliament or a State Legislature shall not be denied to any person.[1]

Read structurally, the clause performed three distinct filtering operations, applied in sequence. The first was a relevance filter: the information had to bear no relationship to any public activity or interest. Information about a public servant's official conduct, expenditure of public funds, or exercise of statutory power failed this filter at the threshold and was therefore never "personal information" of the exempt kind at all. The second was a harm filter: disclosure had to constitute an unwarranted invasion of privacy, the adjective "unwarranted" importing an assessment of proportionality between the intrusion and its occasion. The third was an override: even where the first two filters were satisfied, the information officer retained a duty to disclose if satisfied that the larger public interest justified it. The proviso supplied an external benchmark, anchoring the citizen's entitlement to that of a legislator.

Three features of this design deserve emphasis. First, the clause was conditional rather than categorical: it did not exempt a class of information but a class of circumstances. Second, it distributed judgment rather than concentrating it, requiring an officer to articulate reasons capable of appellate scrutiny by the First Appellate Authority and thereafter by the Information Commission. Third, it embedded within a transparency statute a privacy calculus of some sophistication, well before the Supreme Court held informational privacy to be a facet of Article 21.[2] Whatever the failings of its application — and the record of application was uneven — the clause was, as a matter of statutory craft, a balancing instrument.

3. The Textual Displacement Effected by Section 44(3)

Section 44(3) of the DPDP Act substitutes for the whole of the above the words: "information which relates to personal information". Both the relevance filter and the harm filter disappear. So does the

[1] Right to Information Act 2005, s 8(1)(j) (as originally enacted).

[2] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

public interest override contained within the clause. The proviso, tying citizen access to legislative access, disappears with them.

What survives is Section 8(2) of the RTI Act, which permits a public authority to allow access to exempt information if the public interest in disclosure outweighs the harm to the protected interests, notwithstanding the Official Secrets Act, 1923. It has been argued on behalf of the Union that Section 8(2) preserves the balancing function in substance.[3] The argument is not frivolous, but it is weak for three reasons. First, Section 8(1)(j) imposed a duty on the information officer to disclose where larger public interest justified it; Section 8(2) is permissive in form, conferring a discretion on the public authority. The grammatical shift from obligation to option is not trivial in an administrative culture where refusal is the risk-averse choice. Second, Section 8(2) is addressed to the "public authority" rather than to the Public Information Officer, introducing an ambiguity about who may exercise it at the first instance. Third, and most importantly, the removal of the relevance filter means that the balancing under Section 8(2) now begins from a presumption of exemption rather than from a presumption of disclosure. Under the original clause, information about official conduct never entered the exempt category. Under the amended clause it does, and must be argued out of it.

The consequence is a redistribution of the burden of justification. Before the amendment, an officer refusing information about the assets, disciplinary record or official decisions of a public functionary had to explain why the information bore no relationship to public activity. After the amendment, the citizen must explain why an admittedly "personal" record should nonetheless be released. In a statute whose entire design rests on reversing the colonial presumption of official secrecy, that reversal is significant.[4]

4. Definitional Indeterminacy: An Information-Science Critique

The deeper difficulty is definitional, and it is here that the problem becomes one of information science rather than of constitutional rhetoric alone. The RTI Act does not define "personal information". It defines "information" expansively, as material in any form including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models and data material held in any electronic form.[5] It defines "record" equally broadly.[6] It does not, however, tell an officer what makes information "personal".

The DPDP Act supplies a definition, but of a different term and for a different purpose. "Personal data" is defined as any data about an individual who is identifiable by or in relation to such data.[7] The definition is deliberately capacious, and it is expressly limited to data in digital form or non-digital data subsequently digitised.[8] The RTI Act, by contrast, applies to records in any form whatever. An officer applying the amended Section 8(1)(j) therefore confronts a term that his own statute does not define, whose nearest statutory cognate is both broader in reach and narrower in medium.

Two further asymmetries compound the difficulty. The DPDP Act does not apply to personal data that a data principal has made publicly available, or that any person has made available in compliance with a legal obligation to publish.[9] A great deal of information routinely sought under the RTI Act — electoral affidavits, published seniority lists, gazetted appointments, tender awards — falls within this carve-out and is thus outside the DPDP Act altogether. Yet the amended RTI

[3]This is the substance of the Government's position as advanced during the passage of the Bill: that personal details required to be disclosed under other statutes will continue to be disclosable, and that s 8(2) continues to supply a public interest override.

[4]On the historical inversion of the secrecy presumption effected by freedom of information statutes generally, see Alasdair Roberts, *Blacked Out: Government Secrecy in the Information Age* (Cambridge University Press 2006).

[5]Right to Information Act 2005, s 2(f).

[6]ibid s 2(i).

[7]Digital Personal Data Protection Act 2023, s 2(t).

[8]ibid s 3(a).

[9]ibid s 3(c)(ii).

exemption contains no equivalent carve-out. A provision enacted to align the RTI Act with data protection principles has therefore omitted the very limitation that makes those principles workable.

Second, the amendment is silent on aggregation. Information science has long recognised that records which are individually innocuous may become identifying when combined, and that de-identification is a probabilistic rather than a binary state.[10] This "mosaic effect" is a genuine argument for caution in bulk release, and it is one of the strongest privacy arguments available to the government. But it is an argument for calibrated technique, not for categorical exemption. The RTI Act already contains the appropriate instrument. Section 10 provides for severability, requiring that where a record contains exempt material, access shall nonetheless be provided to that part which does not contain exempt information and which can reasonably be severed.[11] Redaction, pseudonymisation and aggregation to a level at which re-identification risk is acceptable are all available under Section 10. What the amendment does is permit an officer to bypass Section 10 entirely by classifying the whole record as personal at the threshold.

The point may be put in the vocabulary of information governance. Privacy protection in a records system is properly implemented at the level of the record and the field, not at the level of the request. A well-designed public record separates the personal identifier from the administrative fact, so that the fact can be released while the identifier is withheld. The amendment removes the legal incentive to design records in that way, because it makes wholesale refusal lawful and costless. Over time, this is likely to degrade record-keeping practice itself — an institutional cost that will outlast whatever the courts eventually decide.

5. The Judicial Inheritance

The amendment does not operate on a blank slate. Section 8(1)(j) generated a substantial jurisprudence, and much of it is now unsettled.

In *Girish Ramchandra Deshpande v Central Information Commissioner*, the Supreme Court held that a public servant's service record, income tax returns, details of investments and assets, and records of gifts and liabilities were personal information within Section 8(1)(j), disclosure of which had no relationship to any public activity, and that no larger public interest had been shown.[12] The decision has been widely criticised as insufficiently reasoned and as having been applied by information officers as a general immunity for public servants.[13] Nevertheless, its structure is instructive: the Court applied the relevance filter and then considered the override. Both steps existed to be taken.

That structure was elaborated in *CPIO, Supreme Court of India v Subhash Chandra Agarwal*, where a Constitution Bench held that the office of the Chief Justice of India is a public authority under the RTI Act and, more significantly for present purposes, laid down a framework for balancing transparency against privacy.[14] The Court held that the public interest override in Section 8(1)(j) required an assessment of the nature and seriousness of the invasion, the legitimate expectation of the individual, and the value of disclosure to public accountability. It expressly declined to treat the exemption as a class exemption. The reasoning is, in substance, a proportionality analysis conducted within the four corners of the clause.

That reasoning presupposes the clause as it stood. Remove the relevance filter and the internal override, and the analytical hooks on which *Subhash Chandra Agarwal* hangs are gone. It is possible that the Court will read the balancing requirement back in through Section 8(2), or through Articles

---

[10] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA Law Review 1701.

[11] Right to Information Act 2005, s 10(1). The section further requires the officer to give notice of the severance, the reasons for it and the identity of the decision-maker: s 10(2).

[12] *Girish Ramchandra Deshpande v Central Information Commissioner* (2013) 1 SCC 212.

[13] For a representative critique of the mechanical citation of *Deshpande*, see the discussion in *CPIO, Supreme Court of India v Subhash Chandra Agarwal* (2020) 5 SCC 481 [66]–[77].

[14] *CPIO, Supreme Court of India v Subhash Chandra Agarwal* (2020) 5 SCC 481.

19(1)(a) and 21 directly; it is equally possible that information officers, once the provision is notified, will read the amended clause literally. The interim matters, because RTI adjudication is overwhelmingly a first-instance phenomenon and appellate correction is slow.[15]

Underlying all of this is *Puttaswamy*, which supplies both the constitutional foundation of the privacy interest the amendment invokes and the standard by which the amendment must itself be judged. A law limiting a fundamental right must satisfy legality, must pursue a legitimate State aim, must be rationally connected and necessary to that aim, and must strike a proportionate balance, adopting the least restrictive means reasonably available.[16] The legitimate aim of protecting personal data is not in doubt. The difficulty lies at the necessity limb: where a statute already contains a severability mechanism capable of protecting personal data while releasing administrative fact, a categorical exemption is by definition not the least restrictive means.

6. The Constitutional Questions in Prospect

The amendment will be tested once it is notified. It is worth setting out in advance the questions that a challenge would have to raise, since they identify the points at which the drafting is most exposed.

The first is whether Parliament may amend a transparency statute through a data protection statute. There is no inherent constitutional prohibition on amending one enactment by another, and the practice is common. The objection is not to the mode as such but to its consequences for deliberation: an amendment to the principal transparency legislation of the country was carried within a Bill whose subject matter was data protection, and was passed after limited debate. Whether that bears on constitutionality or merely on legislative propriety is itself a question worth argument.

The second is definitional. Does "personal information" in the amended clause take its meaning from Section 2(t) of the DPDP Act, or does it bear an autonomous meaning within the RTI Act? The former reading imports a definition confined to digital data into a statute governing records in every form; the latter leaves the term wholly undefined. Neither outcome is satisfactory, and the choice between them will determine the practical reach of the exemption.

The third is whether the omission of the public interest override survives the proportionality standard. The legitimate aim is not in doubt. The difficulty lies at the necessity limb, for the reason developed in Part 4: Section 10 of the RTI Act already permits the protection of personal particulars by severance while releasing the administrative content of the record. A categorical exemption is, on that footing, not the least restrictive means reasonably available.

The fourth is whether Section 8(2) can bear the balancing weight now placed upon it. That subsection is permissive rather than mandatory, is addressed to the public authority rather than to the information officer, and operates only after the information has been classified as exempt. It is a residual discretion, not a structured test, and it was never designed to carry the entire privacy calculus of the statute.

The fifth concerns Article 19(2). Article 19(2) permits reasonable restrictions on specified grounds; the privacy of a third party is not among them, though "decency" and "defamation" have occasionally been pressed into service. If the right to information is a species of the freedom of expression, traceable to a line of authority beginning with *State of U.P. v Raj Narain*, then a restriction imposed for the protection of another's informational privacy must either be located within an existing head of Article 19(2) or justified through the harmonisation of competing fundamental rights.[17] The latter route requires balancing, which is precisely what the amendment removes from the operative clause.

---

[15] On systemic delay and vacancy in the Information Commissions, see *Anjali Bhardwaj v Union of India* (2019) 18 SCC 246, where the Supreme Court issued directions concerning transparency in appointments and the filling of vacancies.

[16] *K.S. Puttaswamy v Union of India* (2017) 10 SCC 1, particularly the plurality opinion of Chandrachud J and the concurrence of Kaul J; the four-limbed test was applied in *K.S. Puttaswamy v Union of India* (Aadhaar) (2019) 1 SCC 1.

[17] *State of U.P. v Raj Narain* (1975) 4 SCC 428; *S.P. Gupta v Union of India* 1981 Supp SCC 87; *Union of India v Association for Democratic Reforms* (2002) 5 SCC 294.

The sixth is manifest arbitrariness under Article 14. The DPDP Act itself does not apply to personal data made publicly available in compliance with a legal obligation. A provision enacted in the name of that Act, which nonetheless permits refusal of information already required by law to be published, may be said to be irrational on its own terms.

Whether a court would strike the provision down or read it down is a distinct question. The more probable judicial course is reading down: construing “personal information” to exclude information relating to the discharge of public office, and reading Section 8(2) as importing a mandatory balancing exercise. That would preserve the statute while restoring its function. It would also leave the operative text misleading to the officer who must apply it, which is an argument for legislative rather than judicial correction.

7. Comparative Models of Reconciliation

No mature access-to-information regime resolves the transparency–privacy conflict by categorical exemption. Two comparators are instructive.

In the United Kingdom, section 40 of the Freedom of Information Act 2000 exempts personal data of a third party, but only where disclosure would contravene the data protection principles under the Data Protection Act 2018 and the UK GDPR. The practical effect is that the public authority must conduct a legitimate-interests assessment, weighing the interest in disclosure against the reasonable expectations of the data subject and the intrusiveness of release.[18] The exemption is thus conditional on an outcome of balancing, not a substitute for it.

In the European Union, Regulation 1049/2001 on access to documents provides that access shall be refused where disclosure would undermine the protection of privacy and the integrity of the individual, in accordance with Union data protection legislation.[19] In *Commission v Bavarian Lager* the Court of Justice held that the data protection regime applies in full to such requests, requiring the applicant to establish the necessity of transfer.[20] The decision is often described as privacy-protective, and it is; but the mechanism remains an individualised necessity assessment rather than a class exclusion, and later authority has confined it where the personal data is functionally inseparable from the exercise of public functions.

The Council of Europe Convention on Access to Official Documents, the first binding international instrument in the field, likewise permits limitations to protect privacy and other legitimate interests only where the limitation is set down precisely in law, is necessary in a democratic society, and is proportionate; and it requires that access be granted to the remainder of a document where only part is protected.[21] The severability requirement in Article 6(2) is the international analogue of Section 10 of the RTI Act, and its centrality in the Convention scheme confirms that partial disclosure, not categorical refusal, is the internationally accepted technique for reconciling the two interests.

8. Findings and Recommendations

Four findings emerge. First, the amendment effects a structural rather than a cosmetic change: it converts a conditional exemption into a categorical one and relocates the burden of justification from the State to the citizen. Second, it creates a definitional vacuum, importing an undefined term whose nearest statutory analogue is both wider in scope and narrower in medium, and omitting the publicly-available-data carve-out that makes the analogue workable. Third, it is in tension with the necessity limb of the proportionality standard, because Section 10 of the RTI Act already supplies a less restrictive means of protecting personal data. Fourth, it destabilises a body of case law, notably *Subhash Chandra Agarwal*, whose reasoning is keyed to the text now displaced.

[18] Freedom of Information Act 2000 (UK), s 40(2)–(3A), read with the Data Protection Act 2018 and Article 6(1)(f) of the UK GDPR.

[19] Regulation (EC) No 1049/2001, art 4(1)(b); Regulation (EU) 2018/1725 on the protection of personal data by Union institutions.

[20] Case C-28/08 P *European Commission v Bavarian Lager Co Ltd* EU:C:2010:378.

[21] Council of Europe Convention on Access to Official Documents (Tromsø Convention, CETS No 205, adopted 2009, in force 1 December 2020), arts 3 and 6(2).

Five recommendations follow. (i) The most direct legislative remedy is the restoration of the public interest override and the relevance filter within Section 8(1)(j), if necessary in reformulated language drawing on the balancing factors identified in *Subhash Chandra Agarwal*. (ii) Failing repeal, the RTI Act should be amended to define “personal information” autonomously, expressly excluding information relating to the discharge of public office, the expenditure of public funds and the exercise of statutory power, and expressly excluding information already in the public domain by operation of law. (iii) The Department of Personnel and Training should issue binding guidance requiring Public Information Officers to apply Section 10 before invoking Section 8(1)(j), and to record in writing why severance was not reasonably possible. (iv) The Central and State Information Commissions should be directed to report annually on the frequency and outcome of Section 8(1)(j) refusals, generating the empirical record that the present debate conspicuously lacks. (v) At the level of information architecture, public authorities should be required, in their record-management standards, to structure records so that personal identifiers are separable from administrative content — a “disclosure by design” obligation analogous to the privacy-by-design obligations now familiar in data protection practice.

9. Conclusion

The question raised by Section 44(3) is not whether privacy deserves protection in Indian law; after *Puttaswamy*, that question is closed. The question is whether protection is to be achieved by judgment or by exclusion. The original Section 8(1)(j) chose judgment, and in doing so imposed on the administrative state the discipline of giving reasons. The amended clause chooses exclusion, and in doing so relieves the state of that discipline at exactly the point where accountability is most contested — information about the conduct of those who hold public power.

It is possible that the Supreme Court will restore the balancing function by construction, reading Section 8(2) and Articles 19(1)(a) and 21 together to require what the clause no longer states. That would be a welcome outcome, but it would be a second-best one. Balancing tests work best when they are written into the operative provision, applied by the first-instance decision-maker, and reviewable on the reasons recorded. A right of access that survives only because a constitutional court is willing to rescue it is a fragile right. The better course is legislative: to restore to Section 8(1)(j) the structure that made it, for eighteen years, one of the more thoughtful attempts in comparative practice to hold the right to know and the right to be let alone in a single clause.

Declarations

Conflict of interest: The author declares that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analysed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.