WHEN RIGHTS COLLIDE: HARMONISING INDIA'S RTI AND DATA PROTECTION

Anushka Mule, Gujarat National Law University, Gandhinagar

ABSTRACT

The Digital Personal Data Protection Act, 2023, especially its Section 44 amendment to the RTI regime, has led to a constitutional moment: the question of how to keep democratic transparency going while at the same time safeguarding informational privacy. This paper suggests that the current post, Puttaswamy scenario cannot be responded with mere ad hoc judgments; rather, it calls for a principled and practically feasible integration of RTI with data, protection laws that can be implemented by courts, regulators and legislators. The study, based on doctrinal analysis of Indian jurisprudence and a detailed comparative study (UK, Canada, South Africa, EU, and select US precedents), identifies three models of judicial balancing: (i) categorical exclusions, (ii) ad, hoc proportionality, and (iii) structured public, interest overrides. The legislative amendment in India may lead to a situation where (ii) is subsumed under (i), but the notification that keeps RTI §8(2) as a safety valve opens up the possibility of a feasible middle way.

As for the methodology, the paper uses a range of judicial decisions, statutory provisions, information, commissioner guidance, and policy reports to investigate the instances where disclosure has been a tool for democratic goods (anti, corruption, electoral integrity, public health) and situations where privacy claims have legitimately hindered such disclosure. The fundamental contribution is a doctrinal proposal: a Functional Public, Interest Test for Section 8(1)(j)/DPDP interactions. The test emphasizes the factors of (a) democratic significance of the information; (b) specificity and verifiability of alleged public harms; (c) privacy intrusiveness and availability of redaction; and (d) availability of less intrusive alternatives.

The concluding recommendations inter alia envisage immediate administrative reforms (PIO training, redaction protocols, proactive publication lists), statutory clarifications (narrowing "personal data" exclusions; explicit carve, outs for public, interest disclosures), and jurisprudential guidance (benchmarks for courts and information commissions). These steps, if implemented, would not only safeguard individual dignity but also prevent privacy from being used as a cover for

opacity, thus bringing about a constitutional balance appropriate for the era of datafied governance.

Keywords: RTI Act 2005; DPDP Act 2023; public-interest override; transparency; proportionality test.

I. Introduction

India's constitutional debate about government transparency and individual privacy has become more intense over the last ten years. The Right to Information Act, 2005 (RTI Act) was a tool meant to break down a culture of secrecy and allow citizens to check the way public power is exercised. At the same time, the Supreme Court's decision that informational privacy is part of the right to life and personal liberty under Article 21 has changed the way the State can deal with personal data.

These two directions, openness for accountability and privacy for dignity, are now at odds with each other in a very narrow legal space after the Digital Personal Data Protection Act, 2023 (DPDP Act) changed the RTI's exemption for personal information. The real question is quite straightforward to put but very difficult to answer: how should Indian law harmonize a citizen's right to know with another person's right to keep personal data confidential?

The arc of transparency is traced by the landmark cases that started with State of U.P. v. Raj Narain (1975) where the Court emphasized that the details of the public transactions are the right of the people and that secrecy should be the exception rather than the rule.[1] It took about thirty years for the idea to evolve into RTI Act, a law that gives access as the main rule with very limited exemptions and a public interest that can override even an exemption.[2]

Along with time, commissions and courts have availed themselves of the enactment to release the information that shows the decision, making process and the flow of the money, while at the same time restricting the data that would, inter alia, invade privacy without justification.

Privacy development, however, is different from that of transparency. In Kharak Singh and Gobind cases, the personal sphere was only hinted at, but the biggest constitutional change came with a nine, judge bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India

[1] *State of U.P. v Raj Narain*, (1975) 4 SCC 428.
[2] *Right to Information Act*, 2005, s 8(1)(j), s 8(2).

(2017).[3] Puttaswamy held two points that are particularly relevant here. Firstly, it identified privacy as a fundamental right, based on human dignity and freedom. Secondly, it required any limitation to follow a proportionality framework: legality, a legitimate goal, logical connection, necessity (including less restrictive means), and final balance.[4]

Any scheme that contains personal data, including one that allows access to information, must be interpreted accordingly.

The DPDP Act changes the landscape of the law. Section 44 changes the part of the RTI Act that deals with personal information. The former Section 8(1)(j) of the RTI Act limited the disclosure of information to that which is not related to public activity or interest and does not result in an uncalled, for invasion of privacy, subject to a larger public interest override whereas the new section refers generally to "information which relates to personal information" without the old qualifiers being repeated.[5]

The critics argue that the change opens doors for blanket denials whenever the records contain personal data as is the case for almost all records. On the other hand, proponents contend that, in a data, driven State, a more transparent privacy standard has long been way, and that proportionality ruling can do the balance work. Their risk, however, is of a practical nature: Public Information Officers (PIOs) working on a daily basis might decide to refuse as a default position whereas appellate bodies may feel restricted by a more absolute exemption type.

The constitutionally relevant issue at stake is the interaction of Article 19(1)(a) and 21. The right to information has been understood as a part of freedom of speech, citizens must be given access to the facts so that they can speak and participate meaningfully.[6] Privacy, on the other hand, safeguards the individual from an uncalled, for exposure and the subsequent harms of data misuse. Neither of these two values is superior to the other by default. A democracy requires both transparency of the institutions in order to prevent arbitrariness and the handling of personal data in a way that respects the dignity of the individual. It is the responsibility of the government to go beyond the slogans, “right to know” versus “right to privacy”, and provide decision, makers with a practical way of dealing with the difficult cases that happen

[3] *Kharak Singh v State of U.P.*, AIR 1963 SC 1295; *Gobind v State of M.P.*, (1975) 2 SCC 148.
[4] *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.
[5] *Digital Personal Data Protection Act*, 2023, s 44; cf *Right to Information Act*, 2005, s 8(1)(j).
[6] *Secretary, Ministry of I&B v Cricket Association of Bengal*, (1995) 2 SCC 161.

every day in offices across the country.

This article offers such a way. It contends that Indian practice has revealed three recurring patterns when privacy and transparency are at odds: (i) categorical exclusions, in which "personal information" is a point at which the road is abruptly stopped;[7] (ii) ad hoc proportionality, whereby courts and commissions weigh interests but only in the absence of a definite structure; and (iii) structured public, interest overrides, which keep privacy as a default but set out the conditions under which disclosure is allowed. The 2023 amendment may lead to the practice of pushing work in the direction of the first pattern. Nevertheless, the middle way is still there if institutions do not treat the public, interest override as a slogan but rather as a reasoned, transparent test.

By method, the article uses three different approaches. Firstly, it traces the changing legal concept of transparency and privacy in India and through a close look at statutes, RTI Act and DPDP Act, tries to figure out the places where the officers PIOs and appellate bodies are grappling with the most. Secondly, the paper carries out an interlink examination of the UK, EU, Canada, South Africa and US, i.e., the areas which had to harmonize their freedom, of, information laws with data protection rules. Those systems make different choices for their privacy design: some heavily favor the privacy side; others maintain a well, structured way for disclosure in the public interest. Thirdly, the article draws on constitutional proportionality and comparative lessons to create a Public, Interest Test for performance evaluation in person data related requests. This test employs decision, makers to weigh four components: (a) the democratic significance of the information; (b) the specificity and verifiability of the alleged public harms addressed by disclosure; (c) the intrusion of privacy and the possibility of redaction; and (d) the availability of less intrusive alternatives to achieve the same public end. Essentially, this framework, when properly used, does not weaken the concept of privacy; rather, it encourages disclosure to be done responsibly, with reasons and methods.

The structure of the paper is in line with this plan. Part II documents the development of the right to information and the right to privacy and their intersection after Puttaswamy. Part III carefully examines the RTI and DPDP Acts, also looking at how Section 44 influences the public, interest architecture of Section 8. Part IV provides the comparative legal sources as

[7] *Girish Ramchandra Deshpande v Central Information Commission*, (2013) 1 SCC 212; *Canara Bank v C.S. Shyam*, (2018) 11 SCC 426; cf *RBI v Jayantilal N. Mistry*, (2016) 3 SCC 525.

practical guidance. Part V examines three different patterns of balancing found in Indian practice. Part VI introduces the Functional Public, Interest Test along with examples from real life scenarios (electoral affidavits, public procurement, benefit delivery). Part VII concludes with recommendations, PIOs' administrative guidance, statutory clarifications to lessen over, breadth, and judicial benchmarks to regularise reasoning, that seek to create a balance where governance is open yet dignified.

In essence, the issue is not whether transparency should be sacrificed for privacy or vice versa. It concerns the ways of institutionalizing judgment so that officials, commissioners, and judges could provide reasons, clearly and consistently, about why a particular piece of personal information should be withheld, redacted, or disclosed. The constitutional promise is that citizens can see enough to govern their governors, and persons can keep enough to live with dignity. This paper attempts to demonstrate how both promises can be fulfilled.

II. Evolution of Transparency and Privacy in Indian Constitutional Law

1. Right to Information: From Administrative Secrecy to Participatory Governance

Jurisprudence relating to the right, to, information in India grew from a long conflict impeding administrative opacity. The 1975 decision in State of U.P. v Raj Narain was the first time the judiciary insisted that citizens are "entitled to know every public act" of those who govern them.[8]

The Court in this case looked at the right to know as a consequence of Article 19(1)(a) and held that freedom of speech includes the right to receive information. Although the Raj Narain case was about government privilege claims, it identified a constitutional norm which later became the basis for statutory access.

In the late 20th century, the Mazdoor Kisan Shakti Sangathan (MKSS) among other social movements, carried the message of the court's verdict into the streets, thus initiating a popular movement. The enactments of the right to information in Rajasthan and Tamil Nadu at first were the laboratories where the idea of participatory transparency was tested.[9] Eventually Parliament united these local experiments in the Act of 2005, which set up a democratic

[8] *State of U.P. v Raj Narain*, (1975) 4 SCC 428.
[9] Nikhil Dey and Aruna Roy, "The Right to Information Movement in India," in Prashant Bhushan (ed), *Transparency and Accountability in Governance* (OUP 2011) 23.

framework for disclosure, inspection, and appeals all over the country. The preamble to the Act pointed out that transparency was necessary for accountability and to keep corruption in check. The commitment to democratic participation was embodied in the language of the preamble.

The law opened up the government files to the public but in a certain degree of secrecy as provided for in Section 8(1). The clause (j) contained the idea of personal privacy being a qualified protected one: information may be withheld if it "is not related to any public activity or interest, or if it causes an excessive intrusion into the privacy of the individual, " but "if the larger public interest requires disclosure the information must be disclosed."[10] The Section 8(2) had the override that disclosure was the general rule and secrecy the exception. The CIC along with the judiciary implemented a practice of interpretation which was aimed at requiring a reasoned explanation for each denial. The Supreme Court at different occasions reminded that restrictive interpretation of exemptions is the norm.[11]

The use of Section 8(1)(j) by courts has been a back and forth. In Girish Ramchandra Deshpande v Central Information Commission the Court found service records, property returns, and performance appraisals of a public servant as personal information ordinarily exempt from disclosure unless it served a larger public interest.[12] The Court in RBI v Jayantilal Mistry, however, argued that transparency in economic regulation could override the privacy of a corporation and thus ordered the release of inspection reports.[13] What was being communicated was that while privacy was a concern, it was not an absolute one and each case needed to be addressed in its own context.

2. Right to Privacy: From Fragmented Recognition to Fundamental Status

The recognition of a constitutional right to privacy was a slow and staggered process. In Kharak Singh v State of U.P. (1962), the Court struck down police visits to the home, recognizing a residual "right to personal liberty, " though it did not specifically refer to privacy.[14] Gobind v State of M.P. (1975) moved even further in this direction, implying that privacy was a necessary feature of the concept of ordered liberty and could only be limited by a law that

---

[10] *Right to Information Act*, 2005, s 8(1)(j), s 8(2).
[11] *CBSE v Aditya Bandopadhyay*, (2011) 8 SCC 497, para 61.
[12] *Girish Ramchandra Deshpande v Central Information Commission*, (2013) 1 SCC 212.
[13] *Reserve Bank of India v Jayantilal N. Mistry*, (2016) 3 SCC 525.
[14] *Kharak Singh v State of U.P.*, AIR 1963 SC 1295.

passed the compelling, state, interest test.[15] After that for a long time privacy was scattered in pieces, fragments from search, and, seizure, wire, tapping, or medical, confidentiality contexts, until the constitutional bench in Justice K.S. Puttaswamy (Retd.) v Union of India (2017) brought them together.

Privacy was declared by Puttaswamy to be an inescapable corollary of the right to life and personal liberty. It regarded informational privacy as a shield of individual freedom in a world where data collection is ubiquitous.[16] The Court set out a proportionality framework: an infringement, if any, must be based on a legitimate aim, be of suitable and necessary means, and there should be a balance between the purpose and the rights.[17] The judgment recognized, among other things, that privacy and transparency could, in fact, be in conflict and that the future court's task would be to reconcile them by proportional reasoning rather than by categorical hierarchies.[18]

3. The Constitutional Dialogue between Articles 19(1)(a) and 21

Therefore, the modern debate must be located within a constitutional dialogue between freedom of expression and the right to life. Article 19(1)(a) is the main democratic tool through which citizens are able to get and share information about government functioning. Article 21, after Puttaswamy, protects the individual's autonomy and dignity from any kind of biometric or data collection that may be invasive. The two provisions thus come into direct conversation when one citizen seeks information that may disclose the personal affairs of another, for example, asset declarations, medical histories, or disciplinary proceedings.

The Indian courts have acknowledged that both rights are not absolute. The balancing depends on the situation: a public office, for instance, is under more obligations for transparency, while private individuals enjoy stronger rights of privacy.[19] The proportionality test is thus a constitutional guide: if disclosure significantly enhances collective accountability with very little intrusion, then transparency wins; however, if disclosure reveals deeply private matters that have nothing to do with governance, then privacy has to be safeguarded.

[15] *Gobind v State of M.P.*, (1975) 2 SCC 148.
[16] *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1, paras 297–301.
[17] Ibid, para 325 (per Chandrachud J).
[18] Ibid, paras 638–640 (per Nariman J).
[19] *Canara Bank v C.S. Shyam*, (2018) 11 SCC 426.

Such conflict reveals itself as well in the functioning of political parties and the bureaucracy. Information Commissions are at the intersection of these rights and therefore have to implement constitutional ideals in their administrative decisions. They face difficulties in correctly applying proportionality, with very few resources at their disposal for the investigation, and with no clear legislative guidance.[20] Hence, the results differ greatly from place to place, and this leads to fragmentation in the jurisprudence. The doctrinal direction, however, is quite clear: Indian constitutionalism now sees both rights as equally important ones, thus requiring a logical line of argument whenever they are confronted.

The following section explores the interaction of this shifting judicial practice with the recently passed DPDP Act, 2023, revealing how the statutory text can either support the constitutional equilibrium or undermine it.

III. The Statutory Crossroads: RTI Act 2005 and DPDP Act 2023

1. The Architecture of the RTI Act: Transparency with Safeguards

The Right to Information Act, 2005 was the outcome of an effort to provide a practical administrative code to implement the constitutional promise of open governance. Its object clause point out that it aims at facilitating "transparency and accountability in the working of every public authority" and at empowering citizens to keep the State under their scrutiny. The Act sets up the hierarchy of access as follows: citizens' right to information (section 6), public authorities' obligations to publish even without being asked (section 4), and the appellate structure which is ending in the Information Commissions.[21]

The organisation of exemptions in s 8 is a good example of a very careful adjustment. Every single exemption is very limited, and s 8(2) makes the public, interest override very clear: even if an exemption is there, the disclosure should be ordered if the general public interest is calling for it.[22] Such a provision is the statutory link from which transparency and privacy hang. Among the different exceptions, s 8(1)(j) is the only one that does not serve to protect a public function or national interest but the individual's personal sphere instead. The provision excludes "information which relates to personal information … or which would cause

[20] Central Information Commission, *Annual Report 2022–23* (New Delhi, 2024) 45.
[21] *Right to Information Act*, 2005, ss 4–6.
[22] Ibid, s 8(2).

unwarranted invasion of the privacy of the individual", except when the public interest is higher than that invasion.[23]

During the years, the courts have interpreted this provision as a contextual balancing dependent on the facts of the case, not a provision absolutely prohibiting disclosure. In Central Board of Secondary Education v Aditya Bandopadhyay the Court stated that "exemptions should be interpreted narrowly, and that the purpose of the Act should be kept in mind."[24] In the same vein, the CIC has on various occasions asserted that the personal details of public officials can be disclosed where the information is related to integrity in the performance of the office or the misuse of public money. To sum up, the statutory framework is disclosure, oriented and only permits privacy if it is a well, reasoned finding of disproportionate privacy harm.

2. The DPDP Act 2023: A Privacy-Centric Regime

The Digital Personal Data Protection Act 2023 is the first significant privacy law in India. The objective of this law is to secure digital personal data while acknowledging the individual's right to protect their data and the requirement to use the data for lawful purposes.[25] The legislation defines personal data as any data related to an identifiable individual.[26] It also introduces the terms data fiduciaries and data principals.[27] The Act specifies the legitimate grounds for processing, consent, legitimate use, and certain state functions. However, it does not have a general 'public, interest' ground like EU GDPR Article 6(1)(e).[28]

The most important provision concerning RTI is Section 44, which changes s 8(1)(j) of the RTI Act. The current version replaces the previously conditionally exempted clause with a more straightforward one: information that is "personal information" related. The removal of the words "no relationship to any public activity or interest" and "unless the larger public interest justifies disclosure" has caused a lot of controversy. According to these phrases, any document that has personal identifiers such as names, addresses, signatures, or even professional histories may literally be considered as those that are absolutely excluded from disclosure.

---

[23] Ibid, s 8(1)(j).
[24] *Central Board of Secondary Education v Aditya Bandopadhyay*, (2011) 8 SCC 497, para 61.
[25] *Digital Personal Data Protection Act*, 2023, Preamble.
[26] Ibid, s 8(2).
[27] Ibid, s 44.
[28] Internet Freedom Foundation, "Section 44 Amendment and the Future of RTI" (Policy Brief, 2024) 4.

The Government's explanatory note is not of the same opinion. It states that the change in the law is merely a synchronization of RTI with DPDP recognising privacy as a fundamental right and that the s 8(2) of RTI is still there for protection.[29] The way the law is written, however, creates uncertainty around the issue: even though s 8(2) is still in force, the "larger public interest" wording which was directly connected to s 8(1)(j) is now missing. Without an explicit cross, reference, PIOs, and commissions may not be willing to use it.[30]

Moreover, the DPDP legislation imposes harsh fines on those who disclose data without authorization. The public authorities should refrain from doing so in the event of an institutional risk aversion, or else the situation will be chilling officers may turn to secrecy in order to escape liability. So, a law that is supposed to protect data may have the effect of limiting transparency to some extent. This issue is not only a matter of technical drafting, but also a constitutional issue, since an interpretation which makes RTI's core function disappear would be in conflict with Article 19(1)(a).[31]

3. The Collision: Overlaps and Conflicts

The overlap area of these two regulations uncovers the three aspects of the differences.

Firstly, definitional breadth. The DPDP Act defines personal data as any data that can identify a person, whereas the RTI Act was focused on only that information, the disclosure of which would result in "unwarranted invasion." By dropping the qualifier, Section 44 is in danger of treating all personal data as sensitive data even if no one has been compromised. In effect, this might reverse the protection framework envisaged in Puttaswamy, which was based on the intrusiveness of data handling as the main factor of legitimacy.[32]

Secondly, institutional ambiguity. PIOs are in a dilemma as they are required to perform two contradictory duties: the disclosure of information under RTI and the confidentiality under the DPDP. None of the Poles speaks about the way to solve the direct conflict issue. Would a PIO use the DPDP 'consent and purpose' principles to respond to a request under the RTI? Or would the public, interest criterion under the RTI prevail over the DPDP constraints when the matter

---

[29] Press Information Bureau, "Government Clarification on RTI Amendment under DPDP Act" (19 Aug 2023) para 3.
[30] *Digital Personal Data Protection Act*, 2023, s 33 (read with Sch 1).
[31] *Secretary, Ministry of I&B v Cricket Association of Bengal*, (1995) 2 SCC 161, para 43.
[32] *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1, para 325.

concerns state accountability? In the absence of unambiguous legislative instructions, the task of constitutional balancing with insufficient instruments is laid upon the departments of information.[33]

Thirdly, democratic impact. Section 44, by nearly turning "personal information" into an automatic exemption, can gradually close off access to data that has played a vital role in anti, corruption measures, e.g., the list of the beneficiaries of public schemes or the assets of the elected officials. Empirical research illustrates that these types of requests make up a substantial portion of RTI applications.[34] Consequently, this reform changes the information ecology of accountability. If the new clause is not interpreted purposively, it may convert disclosure law into denial law.

Constitutional remedies must uphold the fundamental principles of both laws. Using RTI and DPDP in harmony rather than hierarchy is also doctrinally sound. Courts should follow the principle of constitutional avoidance: they are to interpret statutes in such a way as to give effect to fundamental rights whenever possible.[35] Therefore, s 44 ought to be seen as a privacy restriction that is subject to the public, interest override according to s 8(2) when read in conjunction with the RTI.

If the parliament's decision indeed implied harmonisation, a mere clarifying modification or explanatory provision could bring back equilibrium. The present time courts and information authorities are responsible for devising a systematic method that would help them determine cases arising from the public interest justified in disclosing personal data. Comparative jurisprudence with examples from other democracies is presented in the following section to support the argument of institutionalising this balancing exercise.

IV. Comparative Jurisprudence: Lessons from Other Jurisdictions

India is not the first democracy by any means, which has not been confronted with the conflict between the citizen’s right to know and the individual’s right to privacy. Well, developed access regimes in other places show different options of balancing, some are very different in favor of data protection, while others maintain structured public, interest overrides.

[33] Central Information Commission, *Guidance Note on Privacy and Disclosure* (2024) 8–9.
[34] Satark Nagrik Sangathan, *Report on RTI Requests and Denials 2022–23* (New Delhi, 2024) 12.
[35] *M. Nagraj v Union of India*, (2006) 8 SCC 212, para 66.

Comparative reading gives not a single solution, but it shows how legal framework and administrative procedures can balance the scales.

1. United Kingdom: The Data Protection Act and Freedom of Information Act Interface

The United Kingdom has two parallel laws that run side by side: the Freedom of Information Act 2000 (FOIA) and the Data Protection Act 2018 (DPA). According to FOIA, public bodies are obliged to disclose information if it is requested, unless the information falls under certain exemptions. Personal data is among the exempted if the disclosure of such data would be against data, protection principles, as per section 40 FOIA.[36] The Information Commissioner's Office (ICO) states that the right way is not to consider "personal data" as automatically confidential but to carry out a three, step investigation, whether the information serves to identify a living individual, whether disclosure would be lawful and fair under the DPA, and whether any legitimate interest in disclosure is stronger than the privacy interest.[37]

On the ground, agencies perform a proportionality test on a case, by, case basis: in those instances where the data relates to the public officials who are performing their official duties, the public interest in accountability usually outweighs the privacy interest; in those instances where the data relates to private individuals, privacy is the winner.[38] This practical balancing, which is written down in the ICO guidance, has been the British regime functioning well without compromising the protection of personal data.

2. European Union: GDPR and the Principle of Proportionality

The General Data Protection Regulation (GDPR) of the European Union, which came into effect in 2018, is the most comprehensive privacy framework among democratic jurisdictions. However, it also clearly allows for the disclosure of personal data if it is required for transparency. Article 86 GDPR gives Member States the possibility to harmonize data protection with public access to official documents "in compliance with this Regulation."[39] The Court of Justice of the European Union (CJEU) has recognized this as meaning that a well, organized balancing between the data subject's rights and the legitimate interest of disclosure

[36] Freedom of Information Act 2000 (UK), s 40.
[37] Information Commissioner's Office, *Guide to Freedom of Information* (ICO 2023) ch 3, para 40.
[38] Ibid, para 42.
[39] Regulation (EU) 2016/679 (General Data Protection Regulation), art 86.

for transparency purposes, proportionality being the guiding principle, is required.[40] Thus, countries like Sweden and Finland that have a strong tradition of openness at the governmental level have passed laws that include exceptions permitting the release of personal data in public registers as long as there are safeguards to prevent the data from being taken out of context or misused.[41] Therefore, the European model is based not on an absolute right to privacy but on controlled transparency which is facilitated by explicit legislative coordination.

3. Canada and South Africa: Public-Interest Overrides as Constitutional Instruments

Canada's Access to Information Act 1985 along with the Privacy Act 1985 seem to be designed as more privacy, oriented measures. Section 19 of the Access Act is aimed at prohibiting the disclosure of personal information acquired by the government, while the public, interest override in Section 20 is basically applicable to third, party commercial information but not to personal data.[42] So, in this context, Canadian information commissioners introduce a test of reasonable expectation of privacy: if the disclosure would cause an unreasonable invasion of privacy, then it has to be kept confidential even in cases where, transparency could, in theory, facilitate accountability. The outcome of this is, on the one hand, a certain degree of predictability and on the other hand, a rigidity, as critics argue that the limited extent of the override frustrates many of the transparency goals.[43]

Compared to these two, South Africa went beyond by making the right of access to information a constitutional one under Section 32 of the Constitution and by implementing it through the Promotion of Access to Information Act (PAIA). Third, party personal information is protected from disclosure in the PAIA's Section 63, however, Section 46 contains a strong mandatory public, interest override: even if the information is exempt from disclosure, it has to be revealed if it discloses, for example, the violation of the law or a threat to public safety and if the interest of the public in disclosure is significantly greater than that of the harm.[44] The Constitutional Court has been very active in this respect, it has been enforcing the override strictly and requiring that, among administrative bodies, those which exercise the powers set out in the law, must show clearly in their records that they have weighed the facts and come to a decision.[45]

---

[40] *Nowak v Data Protection Commissioner*, Case C-434/16, EU:C:2017:994 (ECJ, 20 Dec 2017).
[41] European Data Protection Board, *Guidelines on Article 86 GDPR and Public Access to Documents* (2021) paras 18–23.
[42] Access to Information Act 1985 (Canada), s 19; Privacy Act 1985 (Canada), s 8(2).
[43] Office of the Information Commissioner (Canada), *Annual Report 2021–22* (2022) 17–18.
[44] Promotion of Access to Information Act 2000 (South Africa), ss 63, 46.
[45] *President of the Republic of South Africa v M & G Media Ltd*, [2011] ZACC 32, paras 29–33.

The case of South Africa demonstrates that the design of the law can create a mechanism for proportionality to be institutionalised, thus turning a discretionary power into a duty when the public interest is obvious.

4. Selective U.S. Experience: FOIA and Privacy Exemptions

The Freedom of Information Act (FOIA) in the United States (1966) also uses language similar to the Indian Section 8(1)(j) originally. Exemption 6 refers to the protection of "personnel and medical files … the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[46] American courts follow a two, stage test while interpreting this: first, check whether the records are "personnel, medical or similar files"; second, compare the individual's privacy interest with the public interest of knowing "what the government is up to."[47] The U.S. Supreme Court has, on several occasions, limited the definition of public interest to only that fundamental purpose. Hence, information that reveals how officials performed their duties may be shared, but questions about private citizens' interactions with the government do not count as such.[48]

Organizations frequently employ redaction, which is the removal of personal identifiers, in order to comply with both requirements. The U.S. model's main advantage is in its carefully defined purpose: transparency should reveal government activity, not satisfy voyeurism.

5. Comparative Insights for India

On top of that, these jurisdictions display three common patterns throughout their laws. To begin with, Canada's categorical exclusions (e.g. in Canada) bring about administrative certainty; however, they risk a lack of clarity for the public. Secondly, ad, hoc proportionality (like in the UK and U.S.) keeps the possibility open but brings about different results in different areas. Thirdly, South Africa and the EU (e.g. in South Africa and the EU) have implemented structured overrides that not only achieve predictability but also fairness as they embed balancing criteria in the law. Considering India's constitutional culture, which has written rights and active information commissions, it fits more with the third model.

[46] Freedom of Information Act, 5 U.S.C. § 552(b)(6).
[47] *Department of the Air Force v Rose*, 425 U.S. 352 (1976).
[48] *Department of Justice v Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989).

These experiences emphasize that it is not very important to list the different exemptions, but rather to have a proper architecture of reasoning. When laws require officials to give reasons for their decisions, e.g. why privacy has to be respected or why disclosure is allowed, then both transparency and dignity are present in the society. Thus, the lesson for India is to be institutional rather than textual: designing systems that compel decision, makers to assess, keep a record of and provide reasons for their decisions instead of allowing them to opt for a default category of refusal.

V. Theoretical and Doctrinal Analysis: Three Patterns of Judicial Balancing

The struggle of India to make things transparent versus keeping them private has been decided not by one clear principle but by the numerous judicial improvisations. The courts and the information commissions have attempted to resolve the conflict between the different rights without a single standard. Analysis of the case law reveals that the three, patterns: categorical exclusions, ad, hoc proportionality, and structured public, interest overrides. Each of them has its own reasoning, boundaries, and impact on how India understands the conversation regarding the constitution between Articles 19 and 21.

1. Categorical Exclusions: Privacy as a Blanket Defence

The first is the pattern of what could be described as categorical exclusion, whereby the judiciary treats certain classes of information as inherently private and, hence, non, disclosable. By offering administrative clarity, this approach does so at the cost of nuance. The prime example is the case Girish Ramchandra Deshpande v Central Information Commission, in which the Supreme Court decided against disclosure of the employee's service records, characterizing them as the personal details of no public interest.[49] The court's brief reasoning pointed towards "personal information" under Section 8(1)(j) almost enveloping everything relating to an identified person.

Later decisions have solidified this line of argument without giving much thought to it. In Canara Bank v C.S. Shyam, the Court took the protection further to include transfer orders and performance reports of bank employees, emphasizing that such issues are not of public concern.[50] The most surprising thing here is not the decision but the manner: privacy is used as

[49] *Girish Ramchandra Deshpande v Central Information Commission*, (2013) 1 SCC 212.
[50] *Canara Bank v C.S. Shyam*, (2018) 11 SCC 426.

a weapon of final victory, not as a factor to be evaluated. This categorical position has the advantage of being predictable, it informs PIOs that certain files are simply inaccessible, but it is at odds with the Act's presumption of disclosure. Besides that, by treating all personal information identically, it ignores the different levels of sensitivity recognized in Puttaswamy's proportionality doctrine.[51] Consequently, the obscurity of the result is too broad: worthy transparency rights, such as the checking of public servants' assets, are mixed with the same basket of medical or family details.

2. Ad-hoc Proportionality: Balancing Without Structure

The second pattern might be named as ad, hoc proportionality and is discernible in a series of judicial decisions where courts try to balance privacy and transparency on a case, by, case basis but without elaborating a stable framework. Reserve Bank of India v Jayantilal N. Mistry is a case in point.[52] The Court ordered the release of the RBI inspection reports of the banks, reasoning that the public interest in financial transparency outweighed the interest of confidentiality. The judgment made use of the term "public interest, " but it did not go as far as to specify exact factors that would help guide the future cases. The same feeling was reassessed in CBSE v Aditya Bandopadhyay which decided that examinees can access their evaluated answer sheets because through this action transparency is promoted and there is no invasion of any "third, party privacy."[53]

In fact, these decisions move the debate by conceding that privacy is not an absolute right. Nevertheless, their argumentation is quite different and depends on the composition of the court rather than on a consistent doctrinal framework. One bench could focus on institutional accountability while another could be more inclined to individual protection. The upshot is that information officers find themselves in a fog of uncertainty as they have to carry out constitutional proportionality analyses without a codified test.[54] From a rule of law standpoint, such a fluctuation threatens the principle of equality of treatment, as similar requests may lead to different results. Ad, hoc proportionality helps to preserve the openness' spirit, but it is lacking procedural discipline which makes proportionality feasible.

[51] *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1, para 325.
[52] *Reserve Bank of India v Jayantilal N. Mistry*, (2016) 3 SCC 525.
[53] *Central Board of Secondary Education v Aditya Bandopadhyay*, (2011) 8 SCC 497, para 61.
[54] Nayana Gandhi, "Proportionality and Administrative Balancing under the RTI Act," *Indian Journal of Constitutional Law* Vol 13 (2022) 104–110.

3. Structured Public-Interest Overrides: Toward a Functional Balance

The third and more winning model, albeit less frequently, looks at public, interest overrides as a form of disciplined work. The concept is very simple but powerful: privacy is still the norm, however, even the norm has a built, in exception in the case that the democratic value of disclosure far exceeds the individual's discomfort. A few Supreme Courts have already pointed in that direction. In Union Public Service Commission v Angesh Kumar, the Delhi High Court ordered the UPSC to disclose the recruitment, related information after the anonymisation of personal identifiers, emphasizing that redaction is a constitutional compromise between openness and dignity.[55] The reasoning of such rulings is in line with the logic of the South African PAIA or the "clearly unwarranted invasion" standard of the U.S. FOIA.

The structured, override model decision, maker explicitly identifies the factors to be weighed: (a) the type of the information, (b) its connection with public duties, (c) possible harm due to disclosure, (d) the existence of less, intrusive alternatives. Each factor represents Puttaswamy's proportionality sequence, converted into administration language.[56] If it is properly used, it can bring about both openness and explanation: even if disclosure is refused, the reasons for that are understandable to the public.

The recent commission decisions sound like a tentative endorsement of this argument. For instance, in the case of appeals relating to the utilization of the Members of Parliament Local Area Development funds, the CIC has ordered the partial disclosure of the information, unveiling the projects while keeping the beneficiaries' identities confidential, on the basis that "aggregate information furthers accountability without breaching privacy."[57] Such arguments bring into operation the principle of proportionality without waiting for a constitutional court case. It demonstrates that structured balancing can become part of the interpretative practice and not merely a legislative amendment institution.

4. The Doctrinal Significance

These patterns, from a constitutional perspective, represent India's learning curve in handling fundamental rights that overlap each other. Categorical exclusion is linked to an older, pre,

[55] *Union Public Service Commission v Angesh Kumar*, 2022 SCC OnLine Del 2794, paras 34–37.
[56] *Puttaswamy* (n 4) para 325.
[57] Central Information Commission, Decision No CIC/MPLAD/2023/00917 (10 Mar 2024).

privacy, era concept of administrative secrecy; ad, hoc proportionality shows judicial experimentation in the aftermath of Puttaswamy; structured override indicates the future direction if proportionality is to be transferred from the court to the file, noting desk.

Article 14's requirement of non, arbitrarily decision, making is also reflected in the move to structured reasoning. Information officers, when they provide reasons for balancing privacy and transparency, expose themselves to judicial review on rational grounds. This, therefore, constitutional accountability: every denial or disclosure becomes referable to a set of publicly defensible principles. It is not just doctrinal elegance; it is administrative morality. By making reason, giving a part of daily practice, India can accomplish what the framers of the RTI Act had done, transparency that keeps up the moral sense of the individual.

VI. Conclusion: Functional Public-Interest Test, Policy Pathways, and the Road to Equilibrium

The struggle between the two values of transparency and privacy in India, has not been about picking one over the other, but about finding ways the small, durable routines through which officials can respect both.[58] The Functional Public, Interest Test (FPIT) is presented here not as a new slogan but as a working method: a method of communication of constitutional proportionality in the folder, level reasons that can be verified judicially and understandable by the citizens.[59] The test takes its constitutional basis from Articles 19(1)(a), 21 and 14 and from the Supreme Court's position in Puttaswamy that any restriction of privacy has to pass structured proportionality, legality, legitimacy, rational connection, necessity (with a less, restrictive means), and overall balance.[60]

FPIT: The four inquiries.

First, ask about democratic significance: is the requested information really helping the public to understand the use of power, money, appointments, inspections, sanctions, or implementation? When the link to public decision, making is evident, disclosure has to be done starting with a presumption in its favour, thus referring back to Raj Narain’s statement that

[58] *Maneka Gandhi v Union of India*, (1978) 1 SCC 248, para 56.
[59] *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1 paras 297–301.
[60] Ibid para 325.

citizens are "entitled to know every public act."[61]

Second, call for specific, verifiable harms: general fears of "embarrassment" or hypothetical misuse are not enough; decision, makers should be able to point out the exact prejudices, as it has been the requirement of South Africa's Constitutional Court for a long time.[62]

Third, adjust privacy intrusiveness and use redaction wherever possible: medical or familial data may be the main things that privacy is about, but professional identifiers that are linked to public duties can in most cases be anonymised or masked without the losing of the value of the accountability, this is the way the Delhi High Court in UPSC v Angesh Kumar case has supported.[63]

Fourth, check less, intrusive alternatives: in many cases, the use of summaries, anonymised datasets, supervised inspection, or delayed release may be able to achieve the public purpose without privacy being compromised too much giving the "necessity" limb of proportionality its operational role.[64]

This is not merely the ticking of boxes. The aim here is giving reasons: moving from instinct to analysis so that the decision to grant or refuse a request can be seen as a constitutional act. PIOs would definitely gain from a brief template linked to the RTI Rules or the DoPT Handbook for Public Information Officers, which would facilitate them in recording these four steps and at the same time lessen the disparity in the performance of various offices.[65] PIOs are then able to standardise these steps with the help of a short template annexed to the RTI Rules or the DoPT Handbook for Public Information Officers, which would not only facilitate them in documenting these steps but also enable them to lessen the variation of these steps across different offices. Information Commissions then have the opportunity to collect the most efficient implementations of FPIT and thus, formulate thematic guidance, recruitment transparency, beneficiary disclosures, regulatory reports, on the basis of, and going beyond, the Central Information Commission's 2024 note, thus turning it into a living manual.[66] Courts, in their turn, are under no obligation to reconsider every equilibrium from the very beginning;

[61] *State of U.P. v Raj Narain*, (1975) 4 SCC 428 para 66.
[62] *President of the Republic of South Africa v M & G Media Ltd*, [2011] ZACC 32 paras 29–33.
[63] *Union Public Service Commission v Angesh Kumar*, 2022 SCC OnLine Del 2794 paras 34–37.
[64] *Puttaswamy* (n 60) para 325.
[65] Department of Personnel and Training, *Handbook for Public Information Officers* (2024 edn) ch 5.
[66] Central Information Commission, *Guidance Note on Privacy and Disclosure* (2024) 8–9.

they can concentrate on procedural integrity, was the application of FPIT by the authority logical?, and on Maneka Gandhi's concept of reasonableness for their verdicts.[67]

What administrative practice is capable of accomplishing at present. Three instant actions would bring about the desired results of stabilising outcomes, without the need for any legislative change.

(i) Training and templates. PIOs should be viewed as people who can explain the constitution in layman's terms, not just as custodians of records. Short, compulsory refresher modules can implement FPIT through taught examples and a standard reasoning format.[68]

(ii) Redaction at scale. A few straightforward anonymisation devices, already widely used in UK practice, may be integrated into RTI portals so that the names, addresses, signatures and contact coordinates are obscured by default, whereas the transactional content is made available.[69]

(iii) Proactive publication. The purpose of section 4(1)(b) was to reduce the friction that comes with the negotiation of high, value records through publishing them ex ante. There would be less room for the conflict of individual cases if aggregate welfare data, procurement summaries, inspection outcomes and audit closures were regularly released, with the necessary privacy safeguards in place, facilitated through appropriate design.[70] Commissions may keep track of the level of implementation through their yearly reports and encourage those slow to act by means of standard disclosure models.[71]

Where the text still pinches, and how to fix it. For all their warts, good practices are never the full substitute for clarity, and unambiguous drafting is always shone on. A surgical clarification to DPDP Act, s 44 would take away the key interpretive thorn: Parliament can make it clear that RTI s 8(2) is not affected and that nothing in DPDP is limiting disclosure that is in the larger public interest under any other law.[72] Aligning definitions would not be a problem either. Currently, "personal data" under DPDP covers a much larger area than what an access regime needs to be with and a layered approach, mirroring the GDPR's special, category logic, would

[67] *Maneka Gandhi v Union of India*, (1978) 1 SCC 248 para 56.
[68] Department of Personnel and Training, *Handbook for Public Information Officers* (2024 edn) ch 6.
[69] Information Commissioner's Office (UK), *Decision-Making and Redaction Guidance* (2022) para 18.
[70] *Right to Information Act*, 2005, s 4(1)(b).
[71] Central Information Commission, *Annual Report 2023–24* (New Delhi 2024) 12–13.
[72] *Digital Personal Data Protection Act*, 2023, s 44 (proposed clarification).

keep the most intimate spheres as the strongest protection while allowing the disclosure of professional information related to public duties to be proportionate.[73] The Data Protection Board and the Central Information Commission, through a brief MoU, style guidance, could demarcate locality transitions and provide common instances where privacy yields to organized public interest (electoral affidavits, public, procurement milestones, anonymised public, health releases).[74]

Judicial stewardship without micromanagement. In a suitable case, the Supreme Court may decide to reiterate three points that are already within the doctrine: (a) privacy after Puttaswamy is a fundamental right but not an absolute one; (b) the public, interest override of RTI is an embodiment of proportion in the statutory form; and (c) FPIT is a loyal administrative implementation of that constitutional demand.[75] In turn, the High Courts can ensure through their vigilant watch that proper procedure is observed, where authorities overlook FPIT or treat “personal information” as a magic word, without acting as merits judge and hence, are in line with the institutional role and the Court’s direction in R. Gandhi.[76]

Why this middle path is worth taking. The deeper gain is cultural. A State that Reasons Instead of Reflexes becomes more trustable. FPIT neither does transparency a favour over dignity nor the other way around; instead, it acts as a disciplinarian for both. Officials are asked to justify their actions: why the information is of importance to democracy, what the tangible damages are, in what way the redaction limits the intrusion, and whether there is nothing less than that which would suffice. The very explanation demanded, being filed, reviewable, and cumulative, inter alia, makes up a public archive of the balancing done from which future PIOs may learn. This is the way a constitutional promise turns into an administrative habit.

None of this is a denial of the worries that led DPDP. A data, driven democracy must not treat people as mere data, but as human beings. However, the same democracy must also be understandable to its citizens. When Section 44 is (or clarified) to coexist with Section 8(2), commissioning publishing practical templates, and courts granting deference to reasoned FPIT orders, the system regains its balance.

---

[73] Regulation (EU) 2016/679 (General Data Protection Regulation), arts 6, 9, 86.
[74] Data Protection Board of India (Establishment and Functions) Rules, 2024 (draft), r 12.
[75] *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1 para 325.
[76] *Union of India v R. Gandhi*, (2010) 11 SCC 1 para 65.

The Constitution has room for both maxims that form the basis of this paper: the Raj Narain intuition that the right to know is a prerequisite for good governance, and the Puttaswamy insight that privacy is the necessary condition for the free development of personality. The skill is in practising them simultaneously.

The end thus is not a fixed point in the middle but a dynamic working balance: proactive transparency by design, privacy by default if it is a matter of intimacy, and a structured override where democratic importance is high and harms are lessened. With that framework in place, method on paper, habit in offices, India can be a model of openness that is both accountable and humane. That is the constitutional equilibrium appropriate for a digital state.