IN THE HON'BLE SUPREME COURT OF INDIA

(CIVIL ORIGINAL JURISDICTION)

WRIT PETITION (CIVIL) NO. OF 2026

(*Under Article 32 of the Constitution of India*)

IN THE MATTER OF:

The Reporters' Collective Trust & Anr. …Petitioners

versus

Union of India & Anr. …Respondents

I.A. NO. OF 2026: *Application for Interim Relief*

I.A. NO. OF 2026: *Application for Permission to File Lengthy Synopsis and List Of Dates*

PAPER BOOK

[FOR INDEX: KINDLY SEE INSIDE]

ADVOCATE FOR PETITIONERS: ABISHEK JEBARAJ

BATCH MATTERS

ANNEXURE - D -

Sl No.	ADVOCATE'S CHECK LIST (TO BE CERTIFIED BY ADVOCATE ON RECORD)	INDICATE (YES/NO)
1.	SLP has been filed in Form No. 28 with certificate.	NA
2.	The SLP is as per the provisions of Order XV Rule 1.	NA
3.	The papers of SLP have been arranged as per Order XXI, Rule (3)(1)(f).	NA
4.	A brief list of dates/events has been filed.	YES
5.	Paragraphs and pages of paper books have been numbered consecutively and correctly noted in Index.	YES
6.	Proper and required number of paper books (1 + 1) have been filed.	NA
7.	The particulars of the impugned judgment passed by the court(s) below are uniformly written in all the documents.	NA
8.	In case of appeal by certificate the appeal is accompanied by judgment and decree appealed from and order granting certificate.	NA
9.	The Annexures referred to in the petition are true copies of the documents before the court(s) below and are filed in chronological order as per List of Dates.	YES
10.	The annexures referred to in the petition are filed and indexed separately and not marked collectively.	YES
11.	In Appeal against the order passed in Second Appeal, copies of the orders passed by the Trial Court and First Appellate Court have been filed.	NA
12.	The complete listing proforma has been filled in, signed and included in the paper books.	YES
13.	In a petition (PIL) filed under clause (d) of Rule 12(1) Order XXXVIII, the petitioner has disclosed:	NA
(a)	his full name, complete postal address, e-mail address,	NA

	phone number, proof regarding personal identification, occupation and annual income, PAN number and National Unique Identity Card number, if any;	
(b)	The facts constituting the cause of action;	NA
(c)	The nature of injury caused or likely to be caused to the public;	NA
(d)	The nature and extent of personal interest, if any, of the petitioner(s);	NA
14.	In case of appeals under Armed Forces Tribunal Act, 2007, the petitioner / appellant has moved before the Armed Forces Tribunal for granting certificate for leave to appeal to the Supreme Court.	NA
15.	All the paper books to be filed after curing the defects shall be in order.	YES

I hereby declare that I have personally verified the Writ Petition and its contents, and it is in conformity with the Supreme Court Rules 2013. I certify that the above requirements of this Check List have been complied with. I further certify that all the documents necessary for the purpose of hearing of the matter have been filed.

Abishek Jebaraj
ADVOCATE ON RECORD
AoR Code: 3002

Place: New
Delhi Date:
13.02.2026

RECORD OF PROCEEDINGS

S. NO.	RECORD OF PROCEEDINGS	PAGE NO.
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		

INDEX

Sl. No.	Particulars of Documents	Part I (Contents of Paper Book)	Part II (Contents of Paper Book)	Remarks
(i)	(ii)	(iii)	(iv)	(v)
	Court Fee			
1.	Listing Proforma	A-A1	A-A1	
2.	Cover Page of Paper Book		A2	
3.	Index of Record of Proceedings		A3	
4.	Defect List		A4	
5.	Note Sheet		NSI to _____	
6.	Synopsis & List of Dates	B – Q		
7.	Writ Petition under Article 32 of the Constitution of India along with supporting Affidavit.	1 – 67		
8.	**Annexure P-1:** A true copy of the Freedom of Information Act, 2002 [Repealed] published in the Gazette of India, Extra., Pt. II, S. 1, dt. 7th January, 2003, pp. 1-8.	68 – 75		
9.	**Annexure P-2:** A true copy of the Right to Information Act, 2005 published in the Gazette of India, Extra., Part II, Section 1, dated 21st June, 2005, pp. 1-23, No. 25.	76 – 97		
10.	**Annexure P-3:** A true copy of the Personal Data Protection Bill, 2019 (Bill No. 373 of 2019).	98 – 154		
11.	**Annexure P-4:** A true copy of the Digital Personal Data Protection	155 – 178		

	Bill, 2022.			
12.	**Annexure P-5:** A true copy of The Digital Personal Data Protection Bill, 2023, Bill No. 113 of 2023 dated nil.	179 – 211		
13.	**Annexure P-6:** A true copy of the draft Digital Personal Data Protection Rules, 2025.	212 – 235		
14.	**Annexure P-7:** A true copy of the Notifications No. G.S.R. 843(E) dated 13.11.2025 issued by The Ministry of Electronics and Information Technology.	236		
15.	**Annexure P-8:** A true copy of the Notifications No. G.S.R. 846(E) dated 13.11.2025 issued by The Ministry of Electronics and Information Technology.	237 – 254		
16.	**I.A. No. of 2026:** Application for Interim Relief	255 – 258		
17.	**I.A. No. of 2026:** Application for Permission to file lengthy Synopsis and List of Dates.	259 – 2 62		
18.	Filing Memo	263		
19.	Vakalatnama	264 – 265		
20.	Board Resolution dated 25.01.2026	266 – 267		

FOR FIRST LISTING

SECTION-

The case pertains to (Please tick/ check the correct box):-

□	Central Act: (Title)	Constitution of India
□	Section:	Article 32
□	Central Rule: (Title)	N/A
□	Rule No(s):	N/A
	State Act: (Title)	N/A
□	Section	N/A
	State Rule: Title:	N/A
□	Rule No(s):	N/A
□	Impugned Interim Order: (Date)	N/A
	Impugned Final order/ Decree: Date	N/A
□	High Court: (Name)	N/A
□	Names of Judges:	N/A
□	Tribunal/ Authority: (Name)	N/A
1.	Nature of matter:	Civil
2.(a)	Petitioner/ appellant No. 1:	The Reporters' Collective Trust & Anr.
(b)	e-mail ID:	N/A
(c)	Mobile phone number:	N/A
3.(a)	Respondent No.1:	Union of India
(b)	e-mail ID:	N/A
(c)	Mobile phone number:	N/A
4.(a)	Main category classification:	48
(b)	Sub classification:	4805
5.	Not to be listed before:	N/A
6 (a)	Similar disposed of matter with citation, if any, & case details.	No Similar matter is disposed of.
(b)	Similar pending matter with case details	No Similar matter is pending.

7.	Criminal Matters:		N/A		
(a)	Whether accused/convict has surrendered:			N/A	N/A
(b)	FIR	N/A	Date	N/A	
(C)	Police Station:		N/A		
(d)	Sentence Awarded:		N/A		
(e)	Period of sentence undergone including period of detention /custody undergone:		N/A		
(f)	Whether any earlier case between the same parties is filed.		N/A		
(g)	Particulars of the FIR and Case.		N/A		
(h)	Whether any bail application was preferred earlier and decision thereof.		N/A		
8:	Land Acquisition Matters: N/A				
(a)	Date of Section 4 notification:		N/A		
(b)	Date of Section 6 notification:		N/A		
(c)	Date of Section 17 notification:		N/A		
9.	Tax Matters: State the tax effect:		N/A		
10.	Special Category (first petitioner/appellant only): N/A				
	(i) [x] Senior citizen > years			(ii) [x] SC/ST	
	(iii) [x] Woman/child			(iv) [x] Disabled	
	(v) [x] Legal Aid case			(vi) [x] In custody	
11.	Vehicle Number (in case of Motor Accident Claim matters):		N/A		
12.	Whether there was/is litigation on the same point of law, if yes details thereof.		N/A		

Abishek Jebaraj
Advocate on Record
(Registration no.3002)
[redacted]

Date: 13.02.2026

SYNOPSIS

1. The present writ petition is filed, *inter alia*, to challenge the constitutionality of the Digital Personal Data Protection Act, 2023 ("**DPDP Act, 2023**" or "**the Impugned Act**") and the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules, 2025**" or "**the Impugned Rules**"), both as a whole and, in particular, Sections 5, 6, 8, 10, 18, 19, 36, and 44(3), of the DPDP Act, 2023, and Rules 3, 6, 7, 8, 9, 13, 16, 17, and 23 of the DPDP Rules, 2025. The Ministry of Electronics and Information Technology ("**MeitY**" / "**Respondent No. 1**") notified dates for entry into force of the provisions in the DPDP Act, 2023 and the DPDP Rules, 2025 by Notifications No. G.S.R. 843(E) and G.S.R. 846(E), respectively, both dated 13 November 2025.

2. At the outset, the Petitioners submits that DPDP Act, 2023 and the DPDP Rules, 2025 are in complete contravention of the law laid down by this Hon'ble Court in *Justice K.S. Puttaswamy v. Union of India (I), (2017) 10 SCC 1* ("**K.S. Puttaswamy (I)**"). This is because they substantially *weaken* the fundamental right to information, and freedom of speech and expression protected under Article 19(1)(a) of the constitution of India. The DPDP Act, 2023 and the DPDP Rules, 2025 threaten the full spectrum of journalistic activity carried out by journalists, ground reporters, citizens, whistleblowers, RTI activists, and other stakeholders, and strikes at the core of our democratic framework and runs contrary to the basic tenets of the Constitution of India.

3. Petitioner No. 1, The Reporters' Collective Trust, is a collective of like-minded journalists who collaborate to produce rigorous investigative reporting on matters of public interest. Petitioner No. 2, Nitin Sethi is a senior journalist with over two decades of professional experience, and is one of the trustees of Petitioner No. 1. The investigative work undertaken

by the Petitioners is not carried out in isolation and is fundamentally dependent on the assistance of on-ground reporters, citizens, whistleblowers, RTI activists, and other stakeholders, without whose participation such journalism would be impossible.

4. In particular, the Petitioners' investigations have been made possible through the lawful invocation of the Right to Information Act, 2005. The Petitioner No. 1 and Petitioner No. 2 use the information gathered by researchers, citizens, RTI Activists and Whistleblowers in greater public interest, to write analytical reports publicizing the functioning of the government machinery and ensuring public accountability of the State.

5. Citizens undertaking data gathering or journalistic activities, journalists, or civil society members undertaking journalistic activities handle sensitive personal data such as names of persons securing welfare entitlements, personal data collected to facilitate interventions for vulnerable victims and their rehabilitation, and subscriber/donor information, beneficiary details, and volunteer records. While the DPDP Act, 2023 and DPDP Rules, 2025 do not address any activities that further public purposes including such activities that support journalistic expression, it regulates the underlying processing (e.g., collection, use, storage) of personal data that is inevitable in almost every instance of public accountability mechanisms, including data obtained by citizens to support journalistic expression. This makes both citizens gathering information and journalists who report based on such information subject to onerous obligations under the DPDP Act, 2023 and the DPDP Rules, 2025. The obligations include requirements such as notice and consent for processing personal data, and the need to have personnel to adequately respond to requests for erasure or deletion of data.

6. The primary concern of the Petitioners arises from the need for citizens, on-ground reporters, researchers, RTI activists, civil society organisations,

and other stakeholders who actively assist the Petitioners in producing investigative journalistic reports to also comply with the Impugned Act and the Impugned Rules. Such journalistic reports and their primary data record names and details of persons or entities, within public authorities, who have taken decisions or indulged in any wrong-doing. The Impugned Act and the Impugned Rules force citizens, on-ground reporters, researchers, RTI activists, civil society organisations, and other stakeholders who aid and assist the Petitioners in producing journalistic reports, to provide notice and obtain consent from persons on whom the journalistic report is based. This is counter-productive to the interests of keeping the government and its officials accountable to citizens because it thwarts the ability of citizens to expose wrongdoing of persons in positions of authority.

7. The Petitioner challenges the Impugned Act and Impugned Rules on the following grounds:

    a. Section 44(3) of the DPDP Act, 2023 amending section 8(1)(j) of the Right to Information Act, 2005 ("**RTI Act**") is unconstitutional and manifestly arbitrary. The amendment to the RTI Act in Section 44(3) of the DPDP Act violates freedom of speech and expression and the right to information protected under Article 19(1)(a) of the Constitution of India and is not in pursuit of any of the legitimate aims under Article 19(2). The removal of the public interest override within Section 8(1)(j) of the RTI Act now allows information offices of the government to withhold information that is deemed 'personal' even if it has significant connection to a public activity or public interest. This amendment violates Article 14 and 21 of the Constitution of India because it restricts the right to information in a disproportionate and unreasonable manner. Section 44(3) of the DPDP Act, while ostensibly to 'protect'

E

personal information, actually nullifies the core of the fundamental rights guaranteed under Article 19(1)(a) of the Constitution of India.

b. The DPDP Act has no exemption for processing personal data for public purposes, including in respect of efforts to gather data in the public interest, journalistic expressions. As such, the lack of such an exemption makes the scheme of the DPDP Act unconstitutional, unreasonable and manifestly arbitrary. The lack of a public purpose exemption, including an exemption for journalistic purposes, attracts onerous obligations for citizens undertaking data gathering in the public interest, journalists, and news organizations. If citizens, journalists, media, and citizens who collect data for public purposes, including in support of journalistic expressions, fail to comply with the onerous obligations of data fiduciary, or as the case may be, significant data fiduciary, they may be liable for penalties for the breach of the DPDP Act. Thus, the lack of an exemption for processing personal data for public purposes, including in support of journalistic purposes, directly affects the ability of citizens' freedom of speech and expression, and their ability to hold the government accountable.

c. Section 36 of the DPDP Act read with Rule 23 of the DPDP Rules empowering the central government to call for information is unconstitutional and violates Articles 14, 19 and 21 of the Constitution of India. This provision authorises and facilitates unreasonable digital searches of personal data available with every data fiduciary or intermediary, contrary to Article 21 of the Constitution of India. Section 36 of the DPDP Act is vague, overbroad and arbitrary and the gathering and storage of personal information under this provision violates individual liberty and

security of the person, contrary to Article 14 of the Constitution of India. To the extent that they prevent individuals from learning about disclosure of personal data to a government agency, they also infringe Article 19 of the Constitution of India. These infringements are not demonstrably justified in a free and democratic society.

d. The Data Protection Board lacks independence and restricts freedom of speech and expression by its punitive penalty regime. The Data Protection Board's process of appointing its Chairperson and members raises concerns of executive control and questions regarding its independence and impartiality.

8. The Petitioners have not filed any such similar petition challenging the Impugned Act or the Impugned Rules in this Hon'ble Court or in any other court.

LIST OF DATES

DATE	PARTICULARS
04.12.1994	The Mazdoor Kisan Shakti Sangathan ("**MKSS**") conducted its first *jan sunwai* at Kot Kirana in Pali District, Rajasthan, demanding transparency in the utilisation of development funds, a substantial portion of which was alleged to have been misappropriated by corrupt bureaucrats and government agencies. The campaign sought disclosure of official records, institutionalisation of social audits of government expenditure, and the establishment of effective grievance redressal mechanisms for persons deprived of their lawful entitlements. The jan sunwai marked a significant moment in the grassroots right to information movement and captured the imagination of a wide cross-section of society, including activists, civil servants, and members of the legal fraternity, thereby strengthening the demand for transparency and accountability in public administration.
05.04.1996	Following a series of jan sunwais conducted by the MKSS across the districts of Rajsamand, Pali, Ajmer, and Bhairon, which exposed entrenched and systemic corruption in public administration in the State of Rajasthan, and in the absence of any remedial action by the State Government despite assurances by the then Chief Minister, MKSS announced a sustained dharna (sit-in protest) at Beawar in Ajmer District, Rajasthan. The protest, which commenced on this date, continued for forty days and emerged as a historic milestone in the demand for recognition of the Right to Information. The dharna witnessed unprecedented participation by rural

	communities, with protestors arriving from over 150 villages across Rajasthan. Notably, the protest articulated a novel and transformative demand for access to information by marginalised communities, rather than conventional claims for food, shelter, or wages. During the course of the protest, a memorandum was submitted to the Sub-Divisional Officer, Beawar, demanding disclosure of records relating to local public expenditure. The movement received extensive material and moral support from local communities, including donations of grain, money, food, water, and voluntary services from doctors, vendors, and trade unions. The protest also assumed a distinct cultural character, marked by songs, theatre, poetry, and other forms of popular expression, which amplified its reach and resonance. As the agitation gathered momentum, it attracted national attention, drawing journalists, legislators, artists, and civil society actors from across the country. Senior journalists, including Nikhil Chakravartty, Kuldip Nayar, and Prabhash Joshi, visited Beawar, and a seminal editorial titled "Hum Jaanenge, Hum Jiyenge" ("We will know, we will live") published by Prabhash Joshi in Jansatta became a defining slogan of the Right to Information movement in India, reinforcing the democratic assertion that the right to know is inseparable from the right to live.
01.05.2000	Following the acceleration of the Right to Information movement at both the national and State levels after 1997, and sustained advocacy by the National Campaign for People's Right to Information ("**NCPRI**") as a broad-based platform for securing public access to information, the Government of Rajasthan enacted a law recognising

	the Right to Information on this date. The Rajasthan Right to Information Act, 2000, which entered into force on 26 January 2001, conferred upon citizens a statutory entitlement to seek and receive information across all sectors of governance, marking a significant advancement in institutionalising transparency and accountability in public administration at the State level.
25.07.2000	The Government of India introduced the Freedom of Information Bill, 2000 in the Lok Sabha, proposing to impose a statutory obligation on public authorities to furnish information sought by citizens, thereby marking the first formal legislative attempt at the national level to recognise and regulate public access to information held by the State.
16.12.2002	The Freedom of Information Bill, 2000 was passed by Parliament and enacted as the Freedom of Information Act, 2002. However, the Act was never brought into force, as the Central Government did not notify the date of its commencement in the Official Gazette, resulting in its continued inoperability.
06.01.2003	The Freedom of Information Act, 2002 (Act No. 5 of 2003) received the assent of the President of India and was notified and enacted. The Act was published in the Gazette of India (Extraordinary), Part II, Section 1, dated 07.01.2003. The enactment sought to create a statutory regime governing access to information held by public authorities at the national level. The Act contained an expansive exemption framework under Section 8 of the Freedom of Information Act, 2002. Section 8(1) exempted from disclosure information whose disclosure would prejudicially affect the sovereignty and integrity of India, the security of the State,

	strategic, scientific or economic interests of India, or the conduct of international relations; public safety and order, or the detection, investigation, and prosecution of offences; Centre–State relations; Cabinet papers, including records of deliberations of the Council of Ministers, Secretaries, and other officers; minutes, records of advice, legal opinions, or recommendations made during the decision-making process prior to an executive decision or policy formulation; trade or commercial secrets and information affecting legitimate economic or commercial interests; and information whose disclosure could result in breach of parliamentary or legislative privilege or contravention of a lawful order of a court. Section 8(2) further provided that, subject to national security considerations, information relating to matters occurring more than twenty-five years prior to a request would be disclosed, with the decision of the Central Government being final in case of any dispute regarding computation of the said period. The Freedom of Information Act, 2002 also provided a framework for disclosure of third-party information under Section 11. Section 11(1) of the Freedom of Information Act, 2002 required the Public Information Officer to issue notice to a third party where information treated as confidential by such party was proposed to be disclosed, subject to a public interest override except in cases involving trade or commercial secrets protected by law. Sections 11(2) to 11(4) prescribed the procedure for representation by the third party, timelines for decision-making, and the right of appeal against a decision to disclose such information.
August, 2004	In August 2004, the NCPRI proposed a comprehensive set of amendments to the Freedom of Information Act, 2002. These

	proposals were aimed at strengthening the statutory framework for access to information and addressing the deficiencies that had prevented the effective operation of the Freedom of Information Act, 2002. The National Advisory Council (NAC) examined these recommendations and endorsed several of the key amendments.
21.06.2005	On 21 June 2005, the Right to Information Act, 2005 (Act No. 22 of 2005) was passed by the Parliament of India and published in the Gazette of India.
28.01.2009	On 28 January 2009, the Unique Identification Authority of India ("**UIDAI**") was notified by the Planning Commission as an authority of the Union Government. UIDAI was established as an attached office of the Planning Commission to implement the Unique Identification project, with the mandate of issuing Unique Identification Numbers (Aadhaar) to residents of India.
18.08.2011	On 18 August 2011, the Government of India stated that it proposed to introduce a Right to Privacy Bill to provide protection to individuals in cases where their privacy is breached through unlawful means. It was clarified that the drafting of the proposed legislation was at a preliminary stage, and that the details of the Bill were yet to be finalised. This statement was made by the Minister of State in the Ministry of Personnel, Public Grievances and Pensions, Shri V. Narayanasamy, in a written reply to a question in the Rajya Sabha.
29.09.2011	The Planning Commission under the chairmanship of Justice A.P. Shah constituted a group of experts committee to analyse the various international privacy principles, national privacy principles and the existing privacy legislations in India.

18.10.2012	On 18 October 2012, Justice K.S. Puttaswamy (Retd.) filed Writ Petition (Civil) No. 494 of 2012 before the Hon'ble Supreme Court of India, challenging the constitutional validity of the Aadhaar Scheme. The petition questioned the legality of the collection and use of biometric data, the absence of a comprehensive legislative framework governing the scheme at the time, and the implications of Aadhaar for the fundamental rights of citizens, particularly the right to privacy.
16.10.2012	On 12 October 2012, an Expert Committee on Privacy, constituted under the erstwhile Planning Commission and headed by Justice A.P. Shah, submitted its report. The report emerged as an influential and foundational document on national and international privacy standards, articulating key principles such as notice, choice and consent, collection limitation, purpose limitation, access and correction, disclosure of information, security safeguards, openness, accountability, and enforcement. The Expert Committee's recommendations significantly shaped subsequent policy and legal discourse on data protection and the right to privacy in India.
18.07.2017	On 18 July 2017, during the hearing in Justice K.S. Puttaswamy (Retd.) and other tagged matters, this Hon'ble Court observed that it had become necessary to authoritatively determine whether the right to privacy is a fundamental right under the Constitution of India. This Hon'ble Court noted that such a determination would require reconsideration of the correctness of earlier Constitution Bench decisions in *M.P. Sharma* v. *Satish Chandra, District Magistrate, Delhi,* 1950 SCR 1077 (Eight-Judge Bench), and *Kharak Singh* v. *State of Uttar Pradesh*, 1962 (1) SCR 332 (Six-Judge Bench), which had held that no such fundamental right existed. Being of the view

	that the issue raised was of substantial constitutional importance, the Court directed that the matter be placed before a nine-judge Constitution Bench, and ordered that the cases be listed on 19.07.2017. Liberty was granted to all parties to file their written submissions in the meantime.
31.07.2017	On 31 July 2017, the Ministry of Electronics and Information Technology (MeitY) constituted an Expert Committee on Data Protection, chaired by Justice B.N. Srikrishna, to examine issues relating to data protection in India and to recommend an appropriate legal framework for the protection of personal data.
24.08.2017	On 24 August 2017, the Supreme Court, in *Justice K.S. Puttaswamy (Retd.)* v. *Union of India (I)*, (2017) 10 SCC 1, authoritatively reaffirmed that the right to privacy is a fundamental right guaranteed under Part III of the Constitution of India. The Court directed the Government to frame a robust data protection regime consistent with the constitutional principles laid down in *K.S. Puttaswamy (I)*. The judgment held that any State action or law infringing the right to privacy must satisfy a three-fold test: (i) legality, i.e., the existence of a valid law; (ii) legitimate State aim, demonstrating a defined and necessary purpose; and (iii) proportionality, requiring a rational nexus between the means adopted and the object sought to be achieved, and the absence of less restrictive alternatives. Further, in the context of Article 21 of the Constitution, the Court clarified that any invasion of privacy must be sanctioned by law and must follow a procedure that is fair, just, and reasonable.

27.07.2018	On 27.07.2018, the ten-member Expert Committee on Data Protection, chaired by Justice B.N. Srikrishna, submitted its 176-page Report to the Ministry of Electronics and Information Technology (MeitY).
26.09.2018	This Hon'ble Court delivered its judgment in *Justice K.S. Puttaswamy (Retd.)* v. *Union of India (Aadhaar-5J)*, (2019) 1 SCC 1, on 26.09.2018, where the majority upheld the constitutional validity of the Aadhaar Act, 2016, while striking down and reading down certain provisions as unconstitutional.
11.12.2019	On 11.12.2019, the Personal Data Protection Bill, 2019 Bill No. 373 of 2019 ("**PDPB, 2019**") was introduced in Parliament. The Bill sought to provide a comprehensive framework for the protection of personal data, regulate the processing of such data by the State, companies, and individuals, and establish a Data Protection Authority. Upon its introduction, the PDPB, 2019 was referred to a Joint Parliamentary Committee comprising members from both Houses of Parliament for detailed examination, review, and to invite suggestions and recommendations on its provisions.
16.12.2021	On 16 December 2021, after nearly two years of deliberations and multiple extensions, the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, submitted its Report. The Report not only examined the PDPB, 2019 but also proposed a substantially revised legislative framework, appending a new draft titled "The Data Protection Bill, 2021, thereby replacing the earlier 2019 Bill with a reworked version of the proposed data protection law.

03.08.2022	On 3 August 2022, the Minister for Communications and Information Technology, Shri Ashwini Vaishnaw, formally withdrew "The Data Protection Bill, 2021" from Parliament, stating that the Government would undertake a comprehensive reconsideration of the data protection framework and introduce a new, comprehensive data protection legislation in place of the withdrawn Bill.
18.11.2022	On 18 November 2022, the Ministry of Electronics and Information Technology (MeitY) published the draft Digital Personal Data Protection Bill, 2022 ("**DPDPB, 2022**"), along with an explanatory note, and invited public comments on the Bill up to 2 January 2023. The public notice accompanying the draft stated that all submissions would be held by the Government in a "fiduciary capacity" and would not be disclosed to the public, purportedly to enable free and frank feedback. While MeitY received comments and subsequently revised the Bill, several core concerns remained unaddressed. These included: (i) wide exemptions proposed for government instrumentalities (notably under provisions corresponding to Clause 18 of the DPDPB, 2022), which could facilitate expanded State surveillance; (ii) a proposed amendment to the Right to Information Act, 2005, particularly Section 8(1)(j), by exempting from disclosure all information containing personal data, thereby substantially diluting the existing public interest test; (iii) the degree of executive control over the Data Protection Board (under provisions relating to its constitution and functioning); and (iv) the imposition of onerous duties and monetary penalties on Data Principals (under clauses dealing with obligations of data principals

	and penalties), without commensurate safeguards against misuse of power by data fiduciaries and the State.
31.01.2023	On 31 January 2023, a batch of petitions challenging the 2016 Privacy Policy of WhatsApp was mentioned before a Constitution Bench of the Supreme Court of India. The matter was placed before a five-judge Bench comprising Justice K.M. Joseph, Justice Ajay Rastogi, Justice Aniruddha Bose, Justice Hrishikesh Roy, and Justice C.T. Ravikumar. During the hearing, the Solicitor General of India, appearing on behalf of the Union of India, informed the Court that a comprehensive Data Protection Bill, after completion of necessary administrative compliances, was proposed to be introduced before Parliament in the second half of the Budget Session, 2023, with the stated objective of creating a statutory framework governing personal data protection in India.
07.08.2023	On 7 August 2023, the Digital Personal Data Protection Bill, 2023 ("DPDPB, 2023") was introduced in the Lok Sabha and taken up for discussion on the same day. The Bill was debated for approximately 52 minutes, with nine Members of Parliament participating in the discussion, and was passed on the same day amid substantial protest and disruption in the House.
09.08.2023	The Digital Personal Data Protection Bill, 2023 ("**DPDPB, 2023**") was introduced in the Rajya Sabha on 9 August 2023. The legislation was passed after approximately one hour and seven minutes of debate, during which seven Members of Parliament spoke on the Bill.
26.03.2025	On 26 March 2025, over 120 Members of Parliament from the INDIA bloc addressed a joint letter to the Minister for Electronics and

	Information Technology and the Union Minister for Information and Broadcasting, Mr. Ashwini Vaishnaw, urging the repeal of Section 44(3) of the Digital Personal Data Protection Act, 2023 ("DPDPA"). The MPs cautioned that Section 44(3) undermines the Right to Information Act, 2005 by effectively removing the public interest test embedded in Section 8(1)(j), thereby diluting the balance between privacy and transparency carefully evolved through statutory design and judicial interpretation. The representation reflects a growing political consensus and echoes long-standing civil society concerns that Section 44(3) strikes at the core of the RTI framework and must be withdrawn to preserve the citizen's right to seek information in matters of public interest.
05.01.2025	On 5 January 2025, the Ministry of Electronics and Information Technology (MeitY) published the draft Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**"), inviting public comments up to 5 March 2025. Subsequently, MeitY refused to disclose copies of the comments received in response to the draft Rules, invoking Section 8(1)(e) of the Right to Information Act, 2005, which exempts from disclosure information held by a public authority in a fiduciary capacity.
13.11.2025	On 13 November 2025, the Digital Personal Data Protection Rules, 2025 were notified and published in the Official Gazette.
	Hence, the present petition

IN THE SUPREME COURT OF INDIA

(CIVIL ORIGINAL JURISDICTION)

WRIT PETITION (CIVIL) NO. OF 2026

(*Under Article 32 of the Constitution of India*)

IN THE MATTER OF:

The Reporters' Collective Trust & Anr. …Petitioner

versus

Union of India & Ors. …Respondents

IN THE MATTER OF:

1. **THE REPORTERS' COLLECTIVE TRUST**
   Through its authorised representative,
   Having its office at: 1/22, Asif Ali Road,
   New Delhi - 110002

…PETITIONER NO. 1

2. **MR. NITIN SETHI**
   S/o K L Sethi
   [redacted]

…PETITIONER NO. 2

versus

1. **UNION OF INDIA**
   Ministry of Electronics and Information Technology (MeitY)

Through the Secretary
Electronics Niketan,
6, CGO Complex,
Lodhi Road, New Delhi - 110003

…RESPONDENT NO. 1

2. **MINISTRY OF LAW & JUSTICE**
Through the Secretary,
4th Floor, A-Wing,
Shastri Bhawan, New Delhi - 110001

…RESPONDENT NO. 2

3. **MINISTRY OF PERSONNEL, PUBLIC GRIEVANCES, AND PENSIONS**
Through the Secretary,
Department of Personnel and Training,
North Block, Central Secretariat,
New Delhi, Delhi 110001

…RESPONDENT NO. 3

(*All are contesting Respondents*)

A WRIT PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA INTER ALIA CHALLENGING THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND DIGITAL DATA PROTECTION RULES, 2025 AND SEEKING ENFORCEMENT OF THE PETITIONERS' RIGHTS GUARANTEED UNDER PART III OF THE CONSTITUTION OF INDIA.

To

The Hon'ble Chief Justice of India

And His Companion Justices of the
Supreme Court of India.

The humble Petition on behalf
of the Petitioner above named.

MOST RESPECTFULLY SHOWETH,

1. The present writ petition is filed, *inter alia*, to challenge the constitutionality of the Digital Personal Data Protection Act, 2023 ("**DPDP Act, 2023**" or "**the Impugned Act**") and the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules, 2025**" or "**the Impugned Rules**"), both as a whole and, in particular, Sections 5, 6, 8, 10, 18, 19, 36, and 44(3), of the Digital Personal Data Protection Act, 2023, and Rules 3, 6, 7, 8, 9, 13, 16, 17, and 23 of the Digital Personal Data Protection Rules, 2025. The Ministry of Electronics and Information Technology ("**MeitY**" / "**Respondent No. 1**") notified the DPDP Act, 2023 and the DPDP Rules, 2025 by Notifications No. G.S.R. 843(E) and G.S.R. 846(E), respectively, both dated 13 November 2025. At the outset, the Petitioners submits that the DPDP Act, 2023 and the DPDP Rules, 2025 substantially *weaken* the fundamental right to information, and freedom of speech and expression protected under Article 19(1)(a) of the constitution of India. The DPDP Act, 2023 and the DPDP Rules, 2025 threaten the full spectrum of activities that are focused on public interest carried out by journalists, ground reporters, citizens, whistleblowers, researchers, RTI activists, civil society organisations, and other stakeholders, and strikes at the core of our democratic framework and runs contrary to the basic tenets of the Constitution of India.

DESCRIPTION OF THE PARTIES

Re. Petitioner No. 1

2. Petitioner No. 1, The Reporters' Collective Trust, is a collective of like-minded journalists who collaborate to produce rigorous investigative reporting on matters of public interest. Petitioner No. 1's work focuses on in-depth research into India's political economy, governance, public policy, and accountability such as issues like women safety, environment, corruption, climate change etc. Petitioner No. 1 publishes its investigations in multiple mediums and languages, often in partnership with other established news organisations. Many of its news reports have been developed on the basis of efforts by citizens, researchers, and civil society organisations to collect information including by querying public authorities using the RTI Act, 2005. The work of Petitioner No. 1 consistently exposes institutional opacity, administrative malpractice, and systemic abuse of power. Its journalistic investigations have sparked parliamentary debates, prompted judicial scrutiny, and catalyzed significant public policy interventions. For this reason, the Petitioner No. 1 was awarded the Appan Menon Memorial Trust award for 2024-2025. Petitioner No. 1 also won the ACJ Investigative Journalism Award 2023, for their three-part series titled "Forests for Profits" by Tapasya and Nitin Sethi which explored gaps in the new forest laws with regard to environmental concerns and tribal community rights.

Re. Petitioner No. 2

3. Petitioner No. 2, Mr Nitin Sethi, is an Indian journalist and a trustee of Petitioner No. 1. He is also a Visiting Faculty member at Ashoka University. He has over two decades of experience in writing, reporting, and investigative journalism. His work focuses on the intersections of India's political

economy, natural resources, environment, climate change, economy, public finance, and development. His reportage has received several prestigious awards, including the Asian College of Journalism Award for Investigative Journalism, 2019 for his article series titled "Paisa Politics", and the Prem Bhatia Award for Environmental Journalism in 2014 for his articles on the environment and development. He has previously held editorial positions at Business Standard, Scroll.in, The Hindu, The Times of India, and Down To Earth. He has also served as Media Lead at the National Foundation for India and as a Partner at Land Conflict Watch. In addition, he has advised several media and non-profit organisations in a pro bono capacity.

Re. Respondent No. 1

4. Respondent No. 1 is the Ministry of Electronics and Information Technology ("**MeitY**"), an executive ministry of the Union of India. MeitY is the nodal ministry responsible for formulating and implementing national policies relating to information technology, electronics, and digital governance. Its mandate includes the development, promotion, and regulation of the electronics and information technology sector in India. MeitY also oversees policy initiatives relating to digital governance, emerging technologies, innovation, and cybersecurity. MeitY undertook public consultations on previous iterations of the data protection law in 2022. MeitY exercises statutory and executive powers in relation to all policy matters relating to information technology, electronics, and internet (other than licensing of internet service providers). As such, this includes data governance and digital regulation, and MeitY is the relevant ministry that is responsible for the enactment, notification, and implementation of the DPDP Act, 2023 and the DPDP Rules, 2025, which are under challenge in the present petition.

Re. Respondent No. 2

5. Respondent No. 2 is the Ministry of Law and Justice ("**MoLJ**"), an executive ministry of the Union of India. It is responsible for legal affairs, legislative functions, and the administration of justice in the country. The Ministry of Law and Justice presently functions through three departments, namely, the Department of Legal Affairs, the Legislative Department, and the Department of Justice. The Legislative Department is responsible for drafting principal legislation for the Union of India. In its capacity as the nodal ministry for legislative drafting and legal advice, Respondent No. 2 is concerned with the enactment, interpretation, and constitutional validity of central legislation, including the DPDP Act, 2023, which is under challenge in the present petition.

STATEMENT OF FACTS

6. The present writ petition raises a challenge to the constitutionality of the DPDP Act, 2023 and the DPDP Rules, 2025. The challenge arises based on the ruling of this Hon'ble Court's judgment in *Justice K.S. Puttaswamy* v. *Union of India (I)*, (2017) 10 SCC 1, which recognised the right to privacy as a fundamental right under Part III of the Constitution, while simultaneously affirming that privacy is not *absolute* and must yield to competing constitutional values, including transparency and the right to information. The Impugned Act and the Impugned Rules are in contravention of the law established by this Hon'ble Court in *Justice K.S. Puttaswamy* v. *Union of India (I)*, (2017) 10 SCC 1 and fundamentally disrupt the balance between privacy and the citizens' right to know. They strike at the core tenet of the Constitution by imperiling the full spectrum of activities that are focused on public interest carried out by journalists, ground reporters, citizens,

whistleblowers, researchers, RTI activists, civil society organisations and other stakeholders.

7. The present challenge concerns the direct and substantial impact by the Impugned Act and the Impugned Rules on the Petitioners' journalistic expression which is based on the ability to collect personal data of many public-minded citizens, researchers, and civil society organisations. Particularly, the ability of the Petitioners to undertake investigative reporting in the public interest, seek information from public authorities, and publish material concerning matters of democratic accountability.

8. The primary concern of the Petitioners arises from the need for citizens, on-ground reporters, researchers, RTI activists, civil society organisations, and other stakeholders who actively assist the Petitioners in producing investigative journalistic reports to also comply with the Impugned Act and the Impugned Rules. Such journalistic reports and their primary data record names and details of persons or entities, within public authorities, who have taken decisions or indulged in any wrong-doing. The Impugned Act and the Impugned Rules forces citizens, on-ground reporters, researchers, RTI activists, civil society organisations, and other stakeholders who aid and assist the Petitioners in producing journalistic reports, to provide notice and obtain consent from persons on whom the journalistic report is based. This is counter-productive to the interests of keeping the government and its officials accountable to citizens because it thwarts the ability of citizens to expose wrongdoing of persons in positions of authority.

9. The Petitioners have bifurcated the factual narrative into two parts:

   A. Legislative and constitutional evolution of the transparency and privacy framework.

B. Public interest journalism and adverse impact on the journalistic activities carried out by journalists with the aid and active support of ground reporters, citizens, whistleblowers, researchers, RTI activists, civil society organisations, and other stakeholders.

A. LEGISLATIVE AND CONSTITUTIONAL EVOLUTION OF THE TRANSPARENCY AND PRIVACY FRAMEWORK

Re. Evolution of the Right to Information in India

10. It is submitted that the Indian constitutional framework has long recognised transparency and access to information as indispensable to democratic governance. Even before the formal enactment of a statutory right to information, this Hon'ble Court in the State *of U.P.* v. *Raj Narain*, AIR 1975 SC 865, [60,63,74] rejected the State's claim of privilege over official documents and held that the right to know the functioning of government flows from Article 19(1)(a) of the Constitution. This Hon'ble Court held that secrecy is an exception and that courts retain the final authority to decide whether disclosure is against public interest. The judgment laid the constitutional foundation of the Right to Information as a facet of free speech. Furthermore, on 30 December 1981, a seven-judge bench of this Hon'ble Court, in *S.P. Gupta* v. *Union of India*, AIR 1982 SC 149, [66-67], authoritatively reaffirmed that the right to information is integral to Article 19(1)(a). This Hon'ble Court rejected blanket claims of confidentiality over official correspondence and held that disclosure is the rule, while non-disclosure must be narrowly justified. This Hon'ble Court observed that transparency is essential to prevent arbitrariness, corruption, and abuse of power.

11. Prior to the enactment of a comprehensive statutory right to information, the industrial disaster at Bhopal on 3 December 1984 exposed the catastrophic consequences of secrecy surrounding industrial safety, environmental risks, and regulatory oversight. The absence of public access to information concerning hazardous technologies and emergency preparedness aggravated the scale of harm. The tragedy demonstrated that, in the absence of legally enforceable information-disclosure mechanisms, affected communities were unable to anticipate, respond to, or seek timely accountability for risks directly implicating life, health, and the environment. This unfortunate disaster triggered demands for transparency and the necessity of public access to information in matters affecting life, health, and the environment.

12. Although this Hon'ble Court had recognised the right to information as an essential facet of Article 19(1)(a), the demand for an enforceable transparency regime had not, for several decades, translated into a nationwide public movement. The Right to Information movement was initiated through the efforts of the Mazdoor Kisan Shakti Sangathan ("**MKSS**"). Rural workers demanded access to official records, including muster rolls relating to public works, to expose systemic corruption. Public authorities resisted disclosure by invoking secrecy. MKSS organised public hearings (Jan Sunwais), which raised voices for accountability and access to information. These mobilisations shifted the conception of the Right to Information from a constitutional principle recognised by this Hon'ble Court to a practical solution of democratic accountability. Civil society initiatives culminated in the preparation of draft Right to Information laws, including a draft proposed in 1993 by the Consumer Education and Research Council, Ahmedabad.

13. In 1996, sustained public agitation led the Government of Rajasthan to constitute a committee to examine public access to administrative records. Around the same time, a national coalition of activists, journalists, lawyers, and former civil servants formed the National Campaign for People's Right to Information ("**NCPRI**"). The NCPRI advocated for a national transparency law and consistently opposed the colonial secrecy framework under the Official Secrets Act, 1923.

14. Several States enacted Right to Information legislation between 1997 and 2001, including Tamil Nadu, Goa, Rajasthan, Karnataka, Delhi, Assam, and Maharashtra. These enactments recognised that access to information is essential for transparency, accountability, and democratic participation, and acknowledged judicial recognition of the right under Article 19(1)(a).

15. The Freedom of Information Act, 2002 (Act No. 5 of 2003) received the assent of the President of India and was notified and enacted. The Act was published in the Gazette of India (Extraordinary), Part II, Section 1, dated 07.01.2003. The enactment sought to create a statutory regime governing access to information held by public authorities at the national level.

    A true copy of the Freedom of Information Act, 2002 [Repealed] published in the Gazette of India, Extra., Pt. II, S. 1, dt. 7th January, 2003, pp. 1-8 is annexed herewith and marked as **Annexure P-1 (Pgs. 68 to 75)**

16. On 21 June 2005, Parliament enacted the Right to Information Act, 2005 ("**RTI Act, 2005**"). The RTI Act, 2005, provided a comprehensive statutory framework to operationalise the fundamental right to information. It reversed the culture of secrecy by mandating disclosure as the norm, subject to narrowly tailored exemptions and public interest overrides provided under Section 8 of the RTI Act. It is submitted that even though the RTI Act

recognised limited privacy-related exemptions under Section 8(1)(j), it did not treat privacy as an overriding or exclusionary value. Instead, the statute adopts a contextual and interest-balancing approach, requiring public authorities to weigh claims of privacy against the public interest in disclosure, particularly where information concerns public functions, misuse of authority, or matters of democratic accountability.

A true copy of the Right to Information Act, 2005 published in the Gazette of India, Extra., Part II, Section 1, dated 21st June, 2005, pp. 1-23, No. 25 is annexed herewith and marked as **Annexure P-2 (Pg. 76 to 97)**

17. The effectiveness of the RTI Act rests on two foundational principles: first, that personal or sensitive information may be disclosed where a demonstrable public interest justifies such disclosure; and second, that public authorities cannot invoke privacy or confidentiality as a blanket cover to shield illegality, corruption, or abuse of power.

18. Investigations into corruption and maladministration often rely on access to records such as personnel files, asset disclosures, inspection reports, file notations, sanction orders, tender documents, and official correspondence. Almost all such records contain some element of personal information. Before the enactment of the DPDP Act, 2023 and DPDP Rules, 2025, such information was disclosable where the public interest in transparency outweighed the individual's privacy interest, as specified in Section 8(1)(j) of the RTI Act. This balancing principle was affirmed by this Hon'ble Court in *Girish Ramchandra Deshpande v. Central Information Commissioner, 2012 AIR SCW 5865, p. 13, where it was recognised that the information can be disclosed if public interest is shown*. Hon'ble Bombay High Court and Delhi High Court respectively in *Surupsingh Hrya Naik v. State of Maharashtra,*

AIR 2007 BOM 121 and V*ijay Prakash v. Union of India, AIR 2010 DELHI 7, have also noted that privacy cannot defeat legitimate claims of accountability*.

Re. Recognition of Privacy as a Fundamental Right in India and Notification of the Impugned Acts and Impugned Rules.

19. On 28 January 2009, the Planning Commission notified the Unique Identification Authority of India ("**UIDAI**") as an authority of the Union Government. UIDAI was established as an attached office of the Planning Commission to implement the Unique Identification project, with the mandate of issuing unique identification numbers, later known as Aadhaar, to residents of India.

20. In September 2010, the Aadhaar programme was formally launched, initially in rural districts of Maharashtra and subsequently expanded across the country. Aadhaar was conceived as a random twelve-digit unique identification number and was projected as a universal proof of identity capable of being linked to passports, Permanent Account Numbers, voter identity cards, bank accounts, driving licences, and other personal records maintained by public and private entities.

21. Although Aadhaar was publicly described as a voluntary scheme, its implementation reflected a sustained effort to render it effectively mandatory. Public authorities and private service providers increasingly required Aadhaar as a precondition for access to essential services and benefits, thereby materially impairing the ability of individuals without Aadhaar to participate fully in social and economic life. The scheme required individuals to part with sensitive personal and biometric information, which was collected and stored in centralised databases under the control of the State.

22. Despite the operational rollout of Aadhaar, the Union Government introduced the National Identification Authority of India Bill, 2010, in Parliament only on 3 December 2010. The National Identification Authority of India Bill, 2010 was referred to the Parliamentary Standing Committee on Finance, which, in its report dated 13 December 2011, recorded serious reservations regarding the legality, necessity, and institutional safeguards of the proposed framework, and found the Bill to be fundamentally deficient. Notwithstanding these findings, the Government did not enact any revised legislation, and the Aadhaar programme continued to operate without a comprehensive statutory framework.

23. Subsequently, on 12 October 2012, an Expert Committee on Privacy, chaired by Justice A.P. Shah and constituted under the Planning Commission, submitted its report. The report articulated foundational privacy and data protection principles, including notice, consent, purpose limitation, collection limitation, security safeguards, accountability, and enforcement, and became a cornerstone for subsequent legal and policy discourse on privacy in India.

24. On 18 October 2012, Justice K.S. Puttaswamy (Retd.) instituted Writ Petition (Civil) No. 494 of 2012 before this Hon'ble Court, challenging the constitutional validity of the Aadhaar scheme. The petition questioned the legality of large-scale biometric data collection in the absence of a statutory framework and alleged violations of fundamental rights, including the right to privacy.

25. Furthermore, on 18 July 2017, during the hearing of the Aadhaar batch of matters, this Hon'ble Court observed that it was necessary to conclusively determine whether the right to privacy constitutes a fundamental right under the Constitution. This Hon'ble Court referred this question to a Nine-Judge

Constitution Bench for reconsideration of earlier judgements of M.P. Sharma and Kharak Singh.

26. While this reference was pending, on 31 July 2017, the Ministry of Electronics and Information Technology constituted an Expert Committee on Data Protection, chaired by Justice B.N. Srikrishna, to examine issues relating to data protection and to recommend a comprehensive legislative framework.

27. On 24 August 2017, the Nine-Judge Constitution Bench of this Hon'ble Court, in *K.S. Puttaswamy (I) (supra)* , unanimously held that the right to privacy is a fundamental right protected under Part III of the Constitution. This Hon'ble Court in *K.S. Puttaswamy (I) (supra), [310],* held that any infringement of privacy must satisfy the tests of legality, the existence of a legitimate State aim, and proportionality.

28. On 27 July 2018, the Justice B.N. Srikrishna Committee submitted its report along with a draft data protection legislation to the Union Government. Furthermore, on 26 September 2018, this Hon'ble Court delivered its judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J), (2019) 1 SCC 1 ("**K.S. Puttaswamy II**")*. The majority upheld the Aadhaar Act, 2016, while striking down or reading down significant provisions. Justice D.Y. Chandrachud dissented, holding the Act unconstitutional in its entirety.

29. On 11 December 2019, the Personal Data Protection Bill, 2019 was introduced in Parliament and referred to a Joint Parliamentary Committee ("**JPC**"). On 16 December 2021, the JPC submitted its report and proposed a substantially revised draft titled the Data Protection Bill, 2021.

A true copy of the Personal Data Protection Bill, 2019 (Bill No. 373 of 2019) is annexed and marked as **Annexure P-3 (Pgs 98 to 154)**

30. On 3 August 2022, the Union Government withdrew the Data Protection Bill, 2021, stating that a fresh and comprehensive data protection legislation would be introduced. On 18 November 2022, the draft Digital Personal Data Protection Bill, 2022, was published for public consultation. The Government stated that public comments would be held in a fiduciary capacity and would not be disclosed.

A true copy of the Digital Personal Data Protection Bill, 2022 is annexed herewith and marked as **Annexure P-4 (Pg. 155 to 178)**

31. On 7 August 2023 and 9 August 2023, respectively, the Digital Personal Data Protection Bill, 2023 was introduced and passed by the Lok Sabha and the Rajya Sabha after limited parliamentary debate. On 11 August 2023, the Impugned Act received assent from the President of India. On 05 January 2025, the Ministry of Electronics and Information Technology published the draft Digital Personal Data Protection Rules, 2025, for public consultation, but subsequently declined to disclose the comments received, invoking Section 8(1)(e) of the RTI Act. On 13.11.2025, the DPDP, 2025 was published in the official gazette.

A true copy of The Digital Personal Data Protection Bill, 2023, Bill No. 113 of 2023 dated nil is annexed herewith and marked as **Annexure P-5 (Pg. 179 to 211)).**

A true copy of the draft Digital Personal Data Protection Rules, 2025 is annexed herewith and marked as **Annexure P-6 (Pg. 212 to 235)**

31. On 13.11.2025, Sections 1(2), 2, 18-26, 35, 38-43, 44(1), and 44(3) of the DPDP Act, 2023 and Rules 1, 2, and 17-21 of the DPDP Rules, 2025 entered into force.

A true copy of the Notifications No. G.S.R. 843(E) dated 13.11.2025 issued by The Ministry of Electronics and Information Technology is annexed herewith and marked as **Annexure P-7 (Pg. 236)**

A true copy of the Notifications No. G.S.R. 846(E) dated 13.11.2025 issued by The Ministry of Electronics and Information Technology is annexed herewith and marked as **Annexure P-8 (Pg. 237 to 254)).**

33. Sections 6(9) and 27(1)(d) of the DPDP Act, 2023 and Rule 4 of the DPDP Rules, 2025 will enter into force on 13.11.2026.

34. Sections 3-5, 6(1)-6(8), 6(10), 7-10, 11-17, 27 (besides 27(1)(d)), 28-34, 36-37, and 44(2) of the DPDP Act, 2023 and Rules 3, 5-16, 22 and 23 of the DPDP Rules, 2025 will enter into force on 13.05.2027.

B. PUBLIC INTEREST JOURNALISM AND IMPACT ON DATA COLLECTION PRACTICES FOR PUBLIC PURPOSE INCLUDING JOURNALISM BY JOURNALISTS, ON GROUND REPORTERS, CITIZENS, RESEARCHERS, WHISTLEBLOWERS, RTI ACTIVISTS, CIVIL SOCIETY ORGANISATIONS AND OTHER STAKEHOLDERS.

35. The Petitioner respectfully submits that the freedom of speech and expression, including the freedom of the press, and right to information are core fundamental rights guaranteed under Article 19(1)(a) of the Constitution of India. This Hon'ble Court has consistently held that a free, independent, fearless, and robust press is essential to constitutional democracy and informed public participation (*Romesh Thappar v. State of Madras, 1950 SCC 436,* [11]; *Sakal Papers (P) Ltd. v. the Union of India 1962 AIR 305,* [28, 37,

41]; *Bennett Coleman & Co. v. Union of India, (1972) 2 SCC 788,* [98]; *S. Khushboo v. Kanniammal, (2010) 5 SCC 600,* [45]; *Shreya Singhal v. Union of India (2015) 5 SCC 1,* [13, 15, 16-24]. The DPDP Act, 2023 and DPDP Rules, 2025, are weakening the substance of the fundamental rights guaranteed under Article 19(1)(a) of the Constitution of India. Journalists, with the aid and active support of on-ground reporters, citizens, researchers, whistleblowers, RTI activists, civil society organisations, and other stakeholders who perform data collection activities for journalistic purposes and exercise freedom of speech and expression, to inform the citizenry and maintain a pluralistic democracy, any legislation guaranteeing the right to privacy should not obliterate the thrust of the rights guaranteed under Article 19(1) or disrupt the basic tenets of the Constitution of India.

36. Investigative journalists associated with Petitioner No. 1 undertake sustained investigative projects and research on matters of public importance. They are actively assisted by on ground reporters, citizens, researchers, whistleblowers, RTI activists, civil society organisations, and other stakeholders perform journalistic activities. These projects are developed over time and published periodically, with subsequent reporting building upon earlier findings. They disseminate their work in multiple regional languages to ensure wider access, inclusivity, and outreach to marginalised and underprivileged communities. Petitioner No. 1 and Petitioner No. 2 (collectively referred to as "**Petitioners**") have written, reported, and investigated extensively on India's political economy, natural resources, environment, climate change, public finance, and development. The groundbreaking work of Petitioners was made possible because of on-ground reporters, citizens, researchers, whistleblowers, RTI

activists, civil society organisations and other stakeholders who were engaging in data collection for holding public authorities accountable.

37. The investigative work undertaken by the Petitioners is not carried out in isolation and is fundamentally dependent on the active assistance of on-ground reporters, citizens, researchers, whistleblowers, RTI activists, civil society organisations, and other stakeholders, without whose participation such journalism would be impossible. These actors help the Petitioners perform their journalistic functions by collecting data through lawful and recognised means, including the use of (i) RTI, (ii) document-based investigations, (iii) source-led reporting, and (iv) independent verification of information in the public interest.

38. Several of these efforts, undertaken through collaborative and lawful means of collecting data for public purposes including for journalistic purposes, have resulted in landmark investigative projects that have brought issues of grave public concern to light. Such investigations have been made possible only through the assistance of on-ground reporters, citizens, whistleblowers, researchers, RTI activists, civil society organisations, and other stakeholders culling out information through RTI or other legally recognised means. The following are illustrative examples of investigations and the documents relied upon therein:

i. "Millions Waiting: One Exam for the Promised Job" authored by Suchak Patel relied on office memoranda from the Dept. of Personnel and Training, Lok Sabha Answers, Booklets prepared by the PIB and their releases, and RTIs to highlight underutilization of the budget of the National Recruitment Agency and other issues such as understaffing. Such research was crucial as this is the agency tasked with conducting a

common eligibility test for multiple positions in the Union Government under a specified level. The Petitioner found that despite having been introduced in 2020, even after 4 years, exams were still not being conducted as exam centers had yet to be finalized.

ii. "In India, an algorithm declares them dead; they have to prove they are alive" by Kumar Sambhav, Tapasya and Divya Joshy, and Tapaya, relied on data presented by the government in the Haryana Sate Assembly, responses by the secretary of the Citizen Resources Information Department, and RTIs filed to show certain shortcomings in the implementation of the Haryana Government's Parivar Pehchan Patra scheme. Important details such as beneficiaries being wrongfully declared dead and incorrect data affecting the algorithm were brought to light. The scheme is intended to ensure that those who depend on government security nets receive the assistance they require and investigative journalism is necessary to highlight where further assistance or effective implementation are needed.

39. The Petitioners submit before this Hon'ble Court that the DPDP Act, 2023, read with the DPDP Rules, 2025, does not provide a clear and effective exemption for activities that support public purposes including journalistic purposes. This spectrum of activities includes information gathered by researchers, citizens, RTI Activists, civil society organisations, and whistleblowers in public interest, and made public through entities such as Petitioner No. 1 and Petitioner No. 2's journalistic expressions undertaken in the public interest.

40. The Petitioners submits that Impugned Act and Impugned Rules fail to provide a clear, workable, and effective exemption for activities that support public purposes including journalistic purposes. Such activities for public purposes include information gathered by any citizen for public interest, researchers, RTI activists, whistleblowers, civil society organisations, and other stakeholders who aid and actively support journalism undertaken in the public interest. The Impugned Act and Impugned Rules impose a chilling effect on investigative journalism by deterring the lawful collection, processing, and publication of information. This chilling effect operates with particular severity upon journalistic expression that is necessarily collaborative in nature and fundamentally dependent on the assistance of on-ground reporters, citizens, researchers, whistleblowers, RTI activists, civil society organisations, and other stakeholders, who act through legally recognised means to collect information regarding the functioning of public authorities.

41. The Petitioner submits that this Hon'ble Court in many cases observed that no law should abridge the exercise of rights under Article 19(1)(a) except in pursuit of any legitimate aim under Article 19(2) of the Constitution of India. The amendment to the RTI Act by Section 44(3) of the DPDP Act is not in the interests of any of the legitimate aims mentioned in Article 19(2) of the Constitution of India, namely, "sovereignty and integrity of India, the security of the State, friendly relations with Foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence".

42. The Petitioner submits that journalists do not operate in isolation. Their investigative journalism is fundamentally dependent on the help of many

persons, without whose participation such reporting would be impossible. The nature of the Petitioners' work necessarily involves the collection of information (including through the RTI Act and other lawful sources), its verification (through documentary records and source-led corroboration), processing, and publication of material relating to corporate entities, public office holders, and bureaucrats. Such activities are undertaken in the public interest and through legally available ways to hold the government. accountable These activities will be directly impaired by the operation of the Impugned Act and Impugned Rules.

43. In the absence of a clear, workable, and effective exemption for public purpose activity including journalistic purposes under the DPDP Act, 2023 and the DPDP Rules, 2025 framed thereunder, such routine functions carried out in the public interest will be construed as breaches of obligations under the DPDP Act, 2023 and DPDP Rules, 2025. The Petitioners' challenge of the DPDP Act, 2023 and DPDP Rules, 2025 is neither academic nor speculative, The Petitioners' challenge to the DPDP Act, 2023 and the DPDP Rules, 2025 is neither academic nor speculative; it goes to the very core of citizens' efforts to keep the government accountable through data collection, and investigative journalism. The investigative work undertaken by the Petitioners and other on-ground reporters, citizens, researchers, whistleblowers, RTI activists, civil society organisations, and other stakeholders demonstrates the manner in which such public-focused activity including journalistic activity will be impacted by the impugned Act and Impugned Rules.

44. Journalism is essential for democratic accountability. The above reports demonstrate how lawful access to official records by citizens, whistleblowers, researchers, RTI activists, civil society organisations, and other stakeholders

enables scrutiny of executive action, exposure of regulatory failure, and disclosure of matters affecting rights, welfare, and governance. The Impugned Act and the Impugned Rules,, by weakening RTI protections and failing to provide a clear public purpose exemption including for journalistic purposes, threatens the ability of citizens to hold the government to account. Such obstruction directly obstructs the Petitioners' exercise of rights under Article 19(1)(a) and undermines the public's right to know. The attack on fundamental rights of the Petitioners is real, immediate, and demonstrable from the Petitioners' past and ongoing work. The present challenge therefore raises issues of grave constitutional importance warranting the intervention of this Hon'ble Court.

45. Accordingly, and in view of the facts and circumstances set out hereinabove, the Petitioners set out the following grounds in support of the present writ petition, without prejudice to one another.

GROUNDS

A. BECAUSE this Hon'ble Court, in the case of *K.S. Puttaswamy (I)*, reaffirmed "privacy" as a fundamental right under Part III of the Constitution of India. This Hon'ble Court, while noting that the Central Government has constituted a Committee chaired by Hon'ble Shri Justice B.N. Srikrishna, former Judge of this Court, for the purpose of developing a data protection framework, directed the Central Government to bring out a robust data protection regime having due regard to the ruling in that case (*K.S. Puttaswamy (I) (supra),* [328]). The DPDP Act and the DPDP Rules are contrary to the ruling of this Hon'ble Court in *K.S. Puttaswamy I (supra).*

B. BECAUSE the purported intention of the provisions in the DPDP Act and DPDP Rules to balance the protection of the right of individuals to protect

their personal data and the need to process personal data for lawful purposes is not achieved through the provisions of the DPDP Act read with the DPDP Rules. The DPDP framework encroaches upon the freedom of speech and expression and the right to information of all speech that serves a journalistic purpose under Article 19(1)(a), 14, and 21 of the Constitution of India.

I. SECTION 44(3) OF THE DPDP ACT AMENDING SECTION 8(1)(J) OF THE RTI ACT IS UNCONSTITUTIONAL AND MANIFESTLY ARBITRARY

C. BECAUSE in *K.S. Puttasamy I (supra)* [325, 377, 419, 526, 565, 629, 639], all opinions accept that the right to privacy is not absolute. The right to privacy must yield in given circumstances when the exercise of other fundamental rights is legitimate and required in state or public interest.

D. BECAUSE the right to information is a fundamental right under Article 19(1)(a) of the Constitution of India, that promotes the transparency and accountability in the working of every public authority. The right to information (variably referred to as, "the right to know") was recognized by the Supreme Court as a component of Article 19(1)(a) of the Constitution of India (*State of U.P. v. Raj Narain*, (1975) 4 SCC 428, [46]; *S.P. Gupta v. Union of India*, (1981) Suppl. SCC 87, [66-67]; *Union of India v. Association of Democratic Reforms*, (2002) 5 SCC 294, [30, 41, 44, 46]; *People's Union for Civil Liberties v. Union of India*, (2004) 2 SCC 476, [45]). The RTI Act, 2005, put in place a practical and accessible regime for citizens to secure access to information under the control of public authorities.

E. BECAUSE the exercise of the rights to freedom of speech and expression and the right to information in the context of journalism involves: (i) every journalist's right to freedom and expression, including their right to receive

information; and (ii) every citizen's right to acquire information. Access to information is essential in a democratic nation, empowering citizens with critical information, and enabling them to consequently make informed choices. In the case of, *Ministry of Information & Broadcasting, Govt. of India v. Cricket Assn. of Bengal*, (1995) 2 SCC 161, [201.1(b)], this Hon'ble Court acknowledged the importance of the State allocating airwaves in such a manner that private entities cannot manipulate news, views, and information, and that they advance the freedom of speech of citizens and ensure plurality and diversity of views, opinions, and ideas. It was noted that this is imperative in every democracy where freedom of speech is assured.

F. BECAUSE the DPDP Act's amendment to the RTI Act directly limits the fundamental right to information under Article 19(1)(a) of the Constitution of India. Section 44(3) of the DPDP Act, 2023 amending Section 8(1)(j) of the RTI Act, 2005 has come into effect on 13 November 2025. Section 8(1)(j) of the RTI Act as amended reads as, "[n]otwithstanding anything contained in this Act, there shall be no obligation to give any citizen, information which relates to personal information". The amended provision removes all the safeguards provided by the original Section 8(1)(j) of the RTI Act. In its unamended form, Section 8(1)(j) of the RTI Act exempted the disclosure of personal information only if such information (a) has no relationship to any public activity or interest, or (b) would cause unwarranted invasion of the privacy of the individual. Notwithstanding the two justifiable reasons for exempting the disclosure of such personal information under Section 8(1)(j) of the RTI Act, the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, allowed disclosure of the information if they are "satisfied" that the larger public

interest justifies the disclosure of such information. This safeguard within Section 8(1)(j) of the RTI Act preserved a discretionary power with the Central Public Information Officer or the State Public Information Officer or the appellate authority to disclose the information, so long as a justifiable reason affecting the larger public interest was present. The removal of the public interest override within Section 8(1)(j) of the RTI Act now allows information offices of the government to withhold information that is deemed 'personal' even if it has significant connection to a public activity or public interest. This is because the amended clause only presents one test before the CPIO, SPIO, or appellate authority, which is whether the information is "personal". The amendment made by Section 44(3) of the DPDP Act to Section 8(1)(j) of the RTI Act drastically weakens the right to information of citizens and journalists. The legal framework for digital personal data protection should not stultify the public's right to information.

G. BECAUSE there is no legitimate aim under Article 19(2) of the Constitution of India that the amendment in Section 44(3) of the DPDP Act ostensibly pursues. The amendment to the RTI Act in Section 44(3) of the DPDP Act is not in the interests of "sovereignty and integrity of India, the security of the State, friendly relations with Foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence". Even if defamation was said to be the purpose behind the amendment, "defamation" is already covered under both civil/tortious liability and criminal liability under Section 356 of the Bharatiya Nyaya Sanhita, 2023. In any case, such protections to the right to reputation have already been recognised by this Hon'ble Court in *Subramanian Swamy v. Union of India, (2016) 7 SCC 221, [198]*.

H. BECAUSE the amendment to Section 8(1)(j) of the RTI Act puts social audits and anti-corruption efforts which are then reported by Journalists at risk by making social welfare schemes and programmes less transparent. In *Supreme Court of India v. Subhash Chandra Agarwal, (2020) 5 SCC 481*, [145], this Hon'ble Court held that the purport of Section 8(1)(j) is to balance privacy with public interest. In doing so, public authorities must identify (*i*) whether there is a reasonable expectation of privacy, and (*ii*) whether on an ultimate balancing analysis, does privacy give way to freedom of expression. However, after the amendment, the prevailing judicial view as to the scope of Section 8(1)(j) of the RTI Act has effectively been legislatively overruled. The approach under Section 44(3) of the DPDP Act threatens both transparency and decision-making based on accurate information and democratic governance as the CPIO may now take help of this definition and refuse information claiming that it is of personal nature. The RTI Act was created to empower citizens and enhance their participation in monitoring public institutions. These changes oppose the original intentions of the RTI Act.

I. BECAUSE the RTI Act powerfully supplemented the transparency provisions and social audit provisions in statutes guaranteeing social welfare. Social audit or public audit is a continuous ongoing process, through which a citizen or a worker can participate in the monitoring and implementation of the rural employment guarantee scheme or public distribution system. It gives any citizen the authenticity, not only to seek information, but also record complaints, suggestions, and demand answers in the public domain. It stands for collective evaluation, and demystifies documents and procedures involved in the implementation of social welfare schemes. The term 'personal data' under the DPDP Act could include names of voters, beneficiaries of welfare

schemes, and people who get subsidies. Presently, social audits carried out under Section 20 of the Viksit Bharat—Guarantee for Rozgar and Ajeevika Mission (Gramin): VB—G RAM G (विकसित भारत—जी राम जी) Act, 2025 (erstwhile, Section 17 of the Mahatma Gandhi National Rural Employment Guarantee Act, 2005) or Section 28 of the National Food Security Act, 2013 at the gram panchayat level, inter-alia, identify the worker's name, work undertaken, number of days of work, and wages paid. Social audit data of various schemes has been made publicly available under the suo-moto disclosures made by public authorities under Section 4(1) of the RTI Act. This is also the basis of press reports on the performance of these programmes. However, the amendment to Section 8(1)(j) of the RTI Act threatens the social audit units' operations. Without an itemised indication of where funds allocated to social welfare programs are being spent, social audits will not provide clear and sufficient understanding of the performance, functioning, and weaknesses of these programs. Weakening these existing mechanisms for holding the government accountable causes harm to vulnerable groups. Additionally, it might no longer be possible to search names in the electoral rolls and other public records such as land records, or company registries.

J. BECAUSE the term "personal information" in Section 44(3) of the DPDP Act is neither defined in the DPDP Act nor in the RTI Act. The DPDP Act defines "personal data" in Section 2(t) as "any data about an individual who is identifiable by or in relation to such data". This is wide enough to include any kind of data relating to an individual. Section 3 of the DPDP Act stated that the scope of the statute only extends to processing of personal data in (i) digital-form, and (ii) non-digital personal data that is subsequently digitized. Section 2(f) of the RTI Act, on the other hand, defines information to mean

"any material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law for the time being in force". As a result, the scope of "information" under the RTI Act is broader than the scope of the kind of personal data covered under the DPDP Act.

K. BECAUSE Section 44(3) of the DPDP Act restricts the right to information in an unreasonable manner. The provisions of fundamental rights in Part III of the Constitution are not independent silos and have to be read together as complementary rights (*Rustom Cavasjee Cooper* v. *Union of India*, (1970) 1 SCC 248, [139-142]; *K.S. Puttaswamy I,* [266-267]*;* and *Maneka Gandhi* v. *Union of India and Anr.*, (1978) 1 SCC 248, [6]). The amendment to Section 8(1)(j) of the RTI Act annuls the citizens' right to information regarding the transparent operation of public affairs. Neither the right to privacy nor the right to protect personal data or personal information justify the infringement of the right to information that helps hold the government accountable. The citizens' right to know and access information is far too important in a democracy, and denying personal information that discloses essential data or particulars about the working of public offices, public authorities, and instrumentalities of the State results in the government operating in secrecy. The amendment to Section 8(1)(j) of the RTI Act threatens the ability of the Indian democracy to hold a plurality and diversity of views, opinions, and ideas (*Ministry of Information & Broadcasting, Govt. of India v. Cricket Assn. of Bengal*, (1995) 2 SCC 161, [201.1(b)]).

L. BECAUSE as observed in *K.S. Puttasamy I (supra),* [325, 377, 419, 526, 565, 629, 639], the right to privacy must yield in given circumstances when dissemination of information or freedom of speech and expression is legitimate and required in state or public interest. Therefore, the right to privacy is to be applied on balancing the said right with social or public interest in the disclosure of certain personal information. *K.S. Puttaswamy I (supra)*, [312] also noted that privacy is not tantamount to secrecy. In the concurring opinion of Justice R.F. Nariman in *K.S. Puttaswamy I (supra),* [495], while considering existing statutory provisions such as Section 8(1)(j) of the RTI Act that defer to the right to privacy in particular contexts, such provisions and their application balance necessities where social or public interests outweigh the particular aspect of privacy claimed. It was also in the interest of balancing competing fundamental rights, namely the right to privacy and the duty of government to effectively operate social welfare schemes, that this Hon'ble Court in *Binoy Viswam v. Union of India, (2017) 7 SCC 59*, [122, 135, 136] upheld the Section 139-AA of the Income Tax Act, 1961, which obligated assessees to provide their Aadhaar number when applying for a PAN card or when filing an income tax return.

M. BECAUSE Section 44(3) of the DPDP Act is manifestly arbitrary and is violative of Article 14 of the Constitution of India. It is now a settled position of law that a statute can be challenged on the ground it is manifestly arbitrary. Article 14 interdicts a provision in a statute when that provision is unreasonable and has a blatantly problematic rationale. Manifest arbitrariness acts as a method to uncover the capricious nature of a law without necessarily having to settle for restrictive methods of constitutional scrutiny. The test of manifest arbitrariness as articulated by Nariman J in *Shayara Bano v. Union*

of India, (2017) 9 SCC 1, [101] states that a law has to be made "capriciously, irrationally and/or without adequate determining principle" for it to be manifestly arbitrary. A law is also manifestly arbitrary when something is done which is "excessive and disproportionate". This standard of manifest arbitrariness was cited with approval by this Hon'ble Court in *Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, [353] and Joseph Shine v. Union of India, (2019) 3 SCC 39, [26-27].* In *Assn. for Democratic Reforms (Electoral Bond Scheme) v. Union of India, (2024) 5 SCC 1, [200-200.2],* Chandarachud CJ, summarized the manner in which this Court has applied the standard of "manifest arbitrariness":

a. A provision lacks an "adequate determining principle" if the purpose is not in consonance with constitutional values. In applying this standard, Courts must make a distinction between the "ostensible purpose", that is, the purpose which is claimed by the State and the "real purpose", the purpose identified by Courts based on the available material such as a reading of the provision; and

b. a provision is manifestly arbitrary even if the provision does not make a classification.

Section 44(3) of the DPDP Act is manifestly arbitrary and is violative of Article 14 of the Constitution of India. This is because Section 44(3) of the DPDP Act, while ostensibly to 'protect' personal information, actually nullifies the core of the fundamental rights guaranteed under Article 19(1)(a) of the Constitution of India. While the protection of personal data and the right to privacy ought to be guaranteed to citizens, Section 44(3) of the DPDP Act does so by stifling the exercise of the freedoms of speech and expression, and the right to information. The Notes on Clauses to the DPDP Act merely states

that Clause 44 provides for amendments related to certain statutes, including the Right to Information Act, 2005. Section 44 of the DPDP Act lacks an "adequate determining principle" to achieve the purpose intended in consonance with constitutional values.

N. BECAUSE Section 44(3) of the DPDP Act is not a proportional restriction on the right to information. Given that there is no established hierarchy between the right to privacy and the right to information, this Hon'ble court will need to adjudicate: (i) Whether the measure is a suitable means for furthering both rights; (ii) whether the measure is least restrictive and equally effective to realise both rights; and (iii) whether the measure has a disproportionate impact on either rights (*Assn. for Democratic Reforms (Electoral Bond Scheme) v. Union of India, (2024) 5 SCC 1*, *[163]*). Section 44(3) of the DPDP Act amends Section 8(1)(j) of the RTI Act effectively nullifying the right to information in respect of personal information in the hands of public authorities, even if that information may serve a public interest in holding the government accountable. The amendment disproportionately curtails the right to information, for the ostensible purpose of protecting personal information and the right to privacy. Moreover, there are less restrictive alternatives to imposing a blanket ban on the disclosure of personal information. The pre-existing Section 8(1)(j) of the RTI Act, notwithstanding certain issues in its implementation, offered a better standard of balancing between the rights to privacy and information. It allowed for a nuanced, case-by-case balancing that prevented arbitrary denials of RTI requests. The amended Section 8(1)(j) of the RTI Act removes this balance and creates a blanket ban, adopts the most restrictive means possible. It presupposes that all "personal information," irrespective of context or public interest value, carries an equal and overriding

privacy concern, which is infeasible and fallacious in a transparent public governance framework.

O. BECAUSE the amendment to Section 8(1)(j) of the RTI Act also deletes the proviso to Section 8(1) of the RTI Act. The proviso stated that any "information which cannot be denied to the Parliament or a State Legislature shall not be denied to any person". This proviso was key to determine information that cannot be denied to citizens, even if they were exempted under any of the clauses of Section 8(1) of the RTI Act. Various High court decisions differed on the point of whether the proviso was only applicable to Section 8(1)(j) or whether it was applicable in respect of all exemptions in Section 8(1) of the RTI Act. While certain High Courts have interpreted this proviso as being applicable only to clause (j) of Section 8(1), namely, the exemption protecting personal information of an individual from disclosure (*Surupsingh Naik v. State of Maharashtra, 2007 SCC OnLine Bom 264*, [14]; *Canara Bank v. Central Information Commission, Delhi, 2007 SCC OnLine Ker 65*, [8]; *University of Calcutta v. Pritam Rooj, 2009 SCC OnLine Cal 318,* p. 31; *Union of India v. Central Information Commission, 2009 SCC OnLine Del 3876*, [41-43]), others have interpreted this proviso as applying to all exemption clauses listed in Section 8(1) (*D.P. Jangra v. State Information Commission, 2011 SCC OnLine P&H 250*, [14]; *Haryana Public Service Commission v. State Information Commissioner,* 2011 SCC OnLine P&H 428, [20]; *Bhupinder Singh Jassal v. State Information Commissioner, Punjab*, *2011 SCC OnLine P&H 3865*, [16, 18]; *Hindu Urban Co-operative Bank Ltd. v. State Information Commission, 2011 SCC OnLine P&H 5581*, [31]). The present writ petitioners respectfully submit that the proviso was in relation to the entirety of Section 8(1), and merely substituting Section 8(1)(j)

through the DPDP Act does not warrant the deletion of the proviso which provided an overriding laid down a threshold to determine the standard of information disclosure. For example, information available to a person in his fiduciary relationship which is exempted under Section 8(1)(e) of the RTI Act, would warrant its disclosure if such information is accessible by a member of the Parliament or the legislatures.

P. BECAUSE while Section 8(2) of the RTI Act remains, it is discretionary and does not offer a better standard of disclosure in comparison to the unamended Section 8(1)(j) of the RTI Act. Section 8(2) of the RTI Act states that public authorities *may* allow disclosure of information where "public interests in disclosure outweighs the harm to the protected interests" even if its disclosure may not be permitted under the Official Secrets Act, 1923 or under the exemptions (including 'personal information' exemption under section 8(1)(j) of the RTI Act). Under the unamended Section 8(1)(j) of the RTI Act, the CPIO, SPIO, or the appellate authority, as the case may be, allowed disclosure of the information if they are "satisfied" that the larger public interest justifies the disclosure of such information. However, Section 8(2) of the RTI Act leaves it to the discretion of public authorities to publish information where public interests in disclosure outweigh the harms to protected interests. In *Supreme Court of India v. Subhash Chandra Agarwal, (2020) 5 SCC 481, [35],* it was noted that the disclosure under Section 8(2) of the RTI Act by the public authority is discretionary, and not a mandate or compulsion.

Q. BECAUSE the "public interest" phrase in Section 8(2) of the RTI Act cannot be used by the CPIO/SPIO who is responding to RTI requests. As observed by this Hon'ble Court in *Supreme Court of India v. Subhash Chandra Agarwal, (2020) 5 SCC 481*, [35] the CPIO/SPIO is under no duty to disclose

information covered by exemptions under Section 8(1) of the RTI Act. Once the CPIO/SPIO comes to the conclusion that any of the exemption clauses is applicable, the CPIO/SPIO cannot pass an order directing disclosure under Section 8(2) of the RTI Act as this discretionary power is exclusively vested with the public authority. The Delhi High Court in *Union of India v. Central Information Commission, 2009 SCC OnLine Del 3876*, [44], also noted that it is not for the CPIO/SPIO to determine that any information covered by the exemption clauses under Section 8(1) of the RTI Act should nevertheless be disclosed under Section 8(2) of the RTI Act. The Delhi High Court noted that unlike the unamended Section 8(1)(j) of the RTI Act, under Section 8(2) of the RTI Act the power to decide whether larger public interest warrants disclosure of information is conferred on the public authority itself, and not the CPIO/SPIO. Thus, Section 8(2) of the RTI Act does not create a vested or justiciable right that the citizens can enforce by an application before the CPIO/SPIO seeking information under the RTI Act.

R. BECAUSE only Central Information Commission ("**CIC**") orders have used the "public interest" requirement in Section 8(2) of the RTI Act to order disclosure of the information. This Hon'ble Court in *RBI v. Jayantilal N. Mistry, (2016) 3 SCC 525*, [78-83], upheld a series of orders of the CIC which had affirmed the disclosure of information pertaining to the Reserve Bank of India on account of its importance for the public interest. Some of the orders that were impugned in that case and upheld therein, used Section 8(2) of the RTI Act to order disclosure of the information, despite the fact that some of the information were within the exemptions under Section 8(1) of the RTI Act (*Jayantilal N. Mistry v. CPIO & Chief General Manager, 2011 SCC OnLine CIC 15841; Kishanlal Mittal v. P. Satish, 2011 SCC OnLine CIC 16327;*

Ashwini Dixit v. Reserve Bank of India, 12 March 2012, Decision No. CIC/SG/A/2011/003293/17640). This shows that it is only when an RTI request is denied by the CPIO/SPIO, the "public interest" requirement in Section 8(2) of the RTI Act is used by CICs to order disclosure of information.

S. BECAUSE even in its unamended form Section 8(1)(j) of the RTI Act was the most commonly used exemption to deny disclosure of information, due to lack of clear definitions for 'personal information', 'public activity', or 'unwarranted invasion'. Two judgments of this Hon'ble Court, namely, *Girish Ramchandra Deshpande v. Central Information Commr., (2013) 1 SCC 212, [12-14]* and *Canara Bank v. C.S. Shyam, (2018) 11 SCC 426, [12-16]*, have interpreted section 8(1)(j) in a manner that restricted the scope of disclosure of information relating to the assets of public servants, their functioning, and performance evaluation. In *Supreme Court of India v. Subhash Chandra Agarwal, (2020) 5 SCC 481, [105-107]*, this Hon'ble Court's decision noted that details of personal assets of judges would not amount to personal information and disclosure of the same would not violate the right to privacy of judges. In that judgment, Justice Khanna's opinion provided an indicative list of what would form part of personal information. This list included aspects such as name, address, physical, mental and psychological status, medical records, treatment, choice of medicine etc. He concluded that such personal information is entitled to protection from unwarranted invasion of privacy and conditional access is available only when stipulation of larger public interest is satisfied. However, the majority decision did not provide adequate guidance on how to determine if the larger "public interest" is satisfied. Ultimately, the decision noted that the satisfaction of the 'public interest' criteria must be determined on a case-to-case basis with public welfare in mind. Hence, even

in its unamended form, section 8(1)(j) of the RTI Act was mired with ambiguity and restrictively interpreted. However, even with its vagueness it still offered a better standard of disclosure than section 8(2).

T. BECAUSE for the above reasons Section 44(3) of the DPDP Act amending Section 8(1)(j) of the RTI Act is unconstitutional and manifestly arbitrary and violative of Articles 14, 19, and 21.

II. THE DPDP ACT HAS NO II. EXEMPTION FOR PROCESSING PERSONAL DATA FOR PUBLIC PURPOSES INCLUDING FOR JOURNALISTIC PURPOSES AND THE SCHEME OF THE DPDP ACT IS UNCONSTITUTIONAL, UNREASONABLE AND MANIFESTLY ARBITRARY

U. BECAUSE the DPDP Act does not exempt the processing of personal data for public purposes, including for journalistic purposes, and the scheme of the DPDP Act in this regard is unreasonable and manifestly arbitrary. In *K.S. Puttaswamy I (supra),* [636, 640], J Kaul noted that while any data protection law should carefully balance privacy concerns and legitimate State interests, including public benefit arising from scientific and historical research based on data collected and processed. J Chandrachud in *K.S. Puttaswamy I (supra),* [311] noted the need for data collection in State planning and to ensure adequate allocation and use of public resources in a social welfare State. In this respect, the judgment recalled the Regulation No. 2016/679 of the European Parliament and of the Council of 27-4-2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive No. 95/46/EC ("**GDPR**"), which recognises competing interests. Such interests include other fundamental rights and public interest including scientific or historical research purposes or statistical purposes.

V. BECAUSE citizens, media, researchers, RTI activists, whistleblowers, journalists, media, and civil society organisations often collect data for public purposes, including for journalistic purposes. They handle sensitive personal data such as names of persons securing welfare entitlements, personal data collected to facilitate interventions for vulnerable victims and their rehabilitation, and subscriber/donor information, beneficiary details, and volunteer records. For example, by surveying RTI applications filed by beneficiaries of the Parivar Pehchan Patra programme who were declared as 'deceased', a journalist member of Petitioner No. 1 had written a report on how beneficiaries of the programme are unable to obtain their social welfare entitlements or effectively gather information on where discrepancies lay through RTIs. While the DPDP Act does not address citizens, researchers, RTI activists, journalists, civil society organisations, or their public purpose activities, including journalistic activities, it regulates the underlying processing (e.g., collection, use, storage) of personal data that is inevitable in almost every instance of public purpose activities including that of journalistic activity.

W. BECAUSE the absence of a public purpose exemption, which includes journalistic purpose exemption, attracts onerous obligations for citizens, researchers, RTI activists, journalists, news organizations, and civil society organisations who collect data to support or assist journalistic expression. Such persons or entities who collect data for journalistic purposes may be construed as data fiduciaries under Section 2(i) of the DPDP Act. Such obligations under Section 8 of the DPDP Act include, (i) giving notice and obtaining consent of data principals for the processing of personal data, (ii) taking reasonable security measures, (iii) delete the personal data when

consent is withdrawn or retention is not necessary, (iv) provide a mechanism for resolving complaints from data principals, (v) offer contact details for addressing data principals' concerns about data processing, and (vi) to give intimation of any data breach to the Data Protection Board and each affected data principal. These requirements are undeniably onerous in the context of processing for public purposes, including for journalistic purposes. Given the nature of the task of keeping the government accountable and the implications for fundamental rights involved, processing personal data for public purposes including for journalistic purposes must be exempted from the provisions of the DPDP Act.

X. BECAUSE citizens, media, researchers, RTI activists, whistleblowers, civil society organizations, and journalists who collect data also face the risk of being classified as a significant data fiduciary. Section 10(1) of the DPDP Act specifies the factors that need to be considered when classifying a data fiduciary or a class of data fiduciaries as significant data fiduciary, which include, (i) the volume and sensitivity of personal data processed, (ii) risk to the rights of Data Principal, (iii) potential impact on the sovereignty and integrity of India, (iv) risk to electoral democracy, (v) security of the State, and (vi) public order. Significant data fiduciaries have additional obligations under Section 10(2) of the DPDP Act such as appointment of a data protection officer, independent data auditor, and undertake measures such as a periodic Data Protection Impact Assessment (DPIA) and an audit once every 12 months.

Y. BECAUSE if citizens, researchers, RTI activists, whistleblowers, journalists, media, civil society organisations and other stakeholders who collect data for journalistic purposes, fail to comply with the onerous obligations of data

fiduciary, or as the case may be, significant data fiduciary, they may be liable for penalties for the breach of the DPDP Act. This will chill investigative journalism and force citizens and journalists to self-censor to avoid massive penalties. Section 33(1) read with the Schedule to the DPDP Act allows imposition of fines on data fiduciaries from Rs. 50 crore up to Rs. 250 crore for non-compliance with various obligations under the DPDP Act. This risk of huge and unaffordable penalties will discourage citizens, civil society organisations, journalists, whistleblowers, researchers, and RTI activists from handling or publishing any personal data, even when public-interest reporting demands it. As a result, individuals with power will evade scrutiny simply by labelling relevant information as "personal information".

Z. BECAUSE save for the draft Digital Personal Data Protection Bill, 2022 and the Digital Personal Data Protection Bill, 2023 as introduced and passed in the Parliament, all prior drafts of India's data protection law made available to the public, specifically exempted compliance with most provisions in DPDPA for processing of personal data for journalistic purposes (See Personal Data Protection Bill, 2018 (contained in Srikrishna Committee Report), s. 47; Personal Data Protection Bill, 2019, s. 3(24) read with 36(e); and the Data Protection Bill, 2021 (contained in the Joint Committee's Report), s.3 (27) read with 36(e)).

AA. BECAUSE other common law countries have also recognized the need for exempting journalistic activities. Exemptions or exceptions for journalistic materials or news activities are provided in the privacy laws of many other countries:

a. The European Union's GDPR enables Member States to provide for exemptions or derogations from certain provisions of the GDPR for

journalistic purposes and freedom of expression (GDPR, art. 85). The provisions from journalists are exempted include, having a lawful reason or basis for using data, providing privacy information, complying with individual rights that people have about their data, etc (GDPR, art. 85).

b. Singapore's Personal Data Protection Act, 2012, in Part II of its First Schedule, provides an exception for news organizations to collect, use, and disclose personal data without consent solely for its news activity.

c. Kenya's Data Protection Act of 2019, in Section 30(1)(b), allows the processing of personal data without the consent of the data principal when required for the purpose of historical, statistical, journalistic, literature and art or scientific research. Section 39 of Kenya's Data Protection Act of 2019 permits the retention of personal data for longer than is "reasonably necessary", when such retention is required for historical, statistical, journalistic literature and art or research purposes.

d. Under Section 7B(4) of Australia's Privacy Act, 1988, acts and practices of 'media organisations' are exempt from the operation of the Act, provided the acts or practices are undertaken 'in the course of journalism' at a time when the organisation is publicly committed to observe standards that deal with privacy. This exemption aims to ensure an appropriate balance between the public interest in freedom of expression and the public interest in adequately safeguarding the handling of personal information.

e. In Canada, the personal information protection principles do not apply to personal information collected, used or disclosed by a private sector organisation for journalistic, artistic or literary purposes (Personal

Information Protection and Electronic Documents Act 2000, SC 2000, c 5, (Canada) ss 4(2)(c), 7(1)(c).).

f. In the United Kingdom, Article 85(1) of the UK's GDPR read with Part 5 of Schedule II to the Data Protection Act, 2018, ensure that the right to protection of personal data is reconciled with the right to freedom of expression and information, by exempting processing for journalistic purposes and for academic, artistic or literary expression and where the data fiduciary reasonably believes that the publication of the material would be in the public interest. When determining "public interest, the Data Protection Act, 2018, requires the data fiduciary to take into account the special importance of public interest in the freedom of expression and information but to have regard to relevant Codes of Practice or guidelines, including that of the BBC Editorial Guidelines, Ofcom Broadcasting Code, IPSO Editors' Code of Practice.

BB. BECAUSE the rights to freedom of speech and expression and the right to information under Article 19(1)(a) of the Constitution of India are rendered meaningless if journalists are effectively forestalled from processing personal data without first complying with impractical and infeasible obligations, and thereby unable to either receive or disseminate information.

CC. BECAUSE for the above reasons, the DPDP framework ought to have a "public purpose" exemption for all citizens who wish to collect, process, and disseminate information for public purposes, including through journalistic expression. Such an exemption needs to be for "public purposes" and not just for the professional class of "journalists". Exemptions from onerous laws like data protection law should be granted based on the activity's function (collecting data for public purposes including data collected for journalistic

expression), and not the identity or professional status of the journalist. This is particularly important today, as the nature of journalism as an activity and profession is radically transforming. The rise of the blogger, photo-journalist, and user-based journalistic activity has become immensely popular among both new and old media companies, a change that has drastically altered the definition of a journalist. Recognizing this, the Court of Justice of the European Union and the European Court of Human Rights, have noted that "journalistic purpose" exemption extends to anyone processing personal data for the sole purpose of disclosing information, opinions, or comments to the public (*Sergejs Buivids v. Datu valsts inspekcija,* Case C–345/17, 14 February 2019; *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Application no. 931/13, 27 June 2017). The GDPR does not define "journalist" and this has allowed the European Court of Human Rights a broad purview to expand the exemption given to journalistic purposes. Thus, to broaden the beneficial nature of the exemption, an exemption from the DPDP Act for all "public purposes" that encompasses journalistic purposes is necessary.

DD. BECAUSE consent withheld by data principals may lead to selective and partial dissemination of information, diluting the strength of the right to information. The DPDPA requires all processing of personal data to proceed on the basis of either consent or when processing is required for certain legitimate uses (e.g., for employment purposes or in the case of a medical emergency) under Section 7 of the DPDP Act. Processing personal data for public purpose activities will invariably fall outside these narrow buckets of "legitimate uses" permitted under Section 7 of the DPPD Act. Even if processing personal data for public purposes was a legitimate use, persons

processing personal data would have to comply with all other obligations of data fiduciaries other than obtaining consent.

EE. BECAUSE obtaining consent at every instance of processing personal data for public purposes including for journalism is an onerous requirement to comply for citizens, researchers, whistleblowers, RTI activists, journalists, civil society organisations, and other stakeholders, undertaking journalistic functions. While certain activities for collection and gathering of data involving interviews, collecting responses to questionnaires, etc., may be covered under Section 7(a) of the DPDP Act, which recognises voluntary provision of personal data by the data principal, most other forms of data collection which informs investigative reports, general news reporting, opinion pieces, analyses, etc., are still largely dependent on private research and investigative study by citizens, researchers, whistleblowers, RTI activists, journalists, civil society organisations, and other stakeholders, which is remarkably absent in the current list of legitimate uses. Given this, citizens, researchers, whistleblowers, RTI activists, journalists, civil society organisations, and other stakeholders, will invariably have to rely upon consent to process any personal data in the course of their journalistic activities. Indeed, the onerous nature of this requirement was critiqued in the Report published by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna titled 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' ("**Srikrishna Committee Report**"). The Committee, which prepared the Personal Data Protection Bill, 2018, noted that mandating consent for processing such personal data would be unfavourable, as the data principal could simply refuse to consent forestalling all such publishing. The fundamental role of the press and its ability to ensure

transparency and accountability would thus be severely undermined by the data principal's ability to simply refuse consent to the processing of their data.

FF. BECAUSE providing a notice to the data principal to obtain consent also necessitates specifying the purpose for processing of personal data, which makes processing for public purposes including for journalistic purposes infeasible. Specifying the purpose for processing personal data, which is a necessary component of a notice to the data principal, is infeasible in the case of data collection activities that are aiding and supporting journalistic activities and may even defeat the purpose of the journalistic activity. For instance, when a journalist is investigating the parties involved in a fraudulent scheme or transaction, reporting on road accidents in a particular city, or publishing information about the achievement of an individual who is a resident of another city, the requirement to provide notice and obtain consent would not only be impractical or infeasible but will likely defeat the purpose of the journalistic endeavour, by causing inordinate delay or impeding the journalist from publishing the news report itself. Moreover, if information pertaining to such fraudulent scheme or transaction was obtained by way of a private citizen, such private citizen may also have to comply with the consent requirement of the Impugned Act, prior to processing personal data to share with journalists like the Petitioners.

GG. BECAUSE informed consent is a core component of data protection regime as recognised in *K.S. Puttaswamy I (supra)*, [298, 307, 521, 525, 637], but such standards of specificity in consent and purpose-based processing should not apply to public purpose activities, including for journalism, which are often exploratory in nature and involve fact-finding exercises. Citizens, researchers, whistleblowers, RTI activists, journalists, civil society

organisations, and other stakeholders, uncover new leads or directions through such research and processing of personal information. It would be impractical for such a person to specify in exact terms the purposes for which the personal data is being collected at such a nascent stage, and unreasonably restrain journalists from fulfilling their professional activities.

HH. BECAUSE while the DPDP Act contains an exemption for processing personal data for research, archiving or statistical purposes under Section 17(2)(b) of the DPDP Act, this exemption is (i) open-ended and subject to onerous standards in Schedule II of the DPDP Rules; (ii) only available where the personal data is not used to 'take a decision specific to the Data Principal', a phrase that is not defined in the DPDP Act and may likely encompass the decision to publish an article or news report about or involving a data principal. Moreover, given that Section 17(2)(b) is in the nature of an exemption, it contains the risk of being interpreted strictly, to exclude *publication* of personal data based on such research, archival, or statistical purpose. For example, whether personal data collected by photo-journalists or photographers, such as images of individuals in a city after a natural calamity would be construed as "personal data for research, archiving or statistical purposes" is unclear. Even if such an image is considered to be exempted, whether publication of that image will be exempted from the onerous obligations under the DPDP Act is also unclear. Accordingly, the exemption for "research, archiving or statistical purposes" likely to be unavailable for processing personal data for journalistic purposes.

II. BECAUSE as per Section 8(3) of the DPDP Act read with Rule 16 and Second Schedule, Para 9(d) of the DPDP Rules, a Data Fiduciary processing personal data is obligated to ensure the data's completeness, accuracy and consistency,

where such data is likely to be used to make a decision that affects the Data Principal or is likely to be disclosed to another Data Fiduciary. This would mean that citizens, researchers, whistleblowers, RTI activists, journalists, media, civil society organisations, and other stakeholders, who are creators online, would have to ensure that their subscribers' data is complete, accurate, and consistent, prior to processing their data for sending email updates to subscribers that have consented to receiving such updates. When the Central Government calls for information pertaining to subscribers under Section 36 of the DPDP Act, journalists will have to ensure that the data that they share is complete, accurate and consistent. The DPDP Act or DPDP Rules do not provide any guidance on how the completeness, accuracy, and consistency of personal data will be verified. In fact, it is the data principal that must seek corrections as required under Section 12 of the DPDP Act. Contrastingly, when the State and its instrumentalities process personal data or when personal data is processed for research, archiving or statistical purposes, the Second Schedule of the DPDP Rules (item (d)) specifies that only "reasonable efforts" need to be taken to ensure the completeness, accuracy, and consistency of personal data. Given the lack of a public purpose exemption, including for journalistic purposes, citizens, researchers, whistleblowers, RTI activists, journalists, civil society organisations, and other stakeholders, will have to mandatorily comply with this requirement of ensuring the completeness, accuracy, and consistency of personal data. Moreover, under Section 8(4) of the DPDP Act, data fiduciaries are expected to implement appropriate technical and organisational measures to ensure the "effective observance" of the DPDP Act and DPDP Rules.

JJ. BECAUSE the DPDP Act, under Section 12, mandates immediate deletion or erasure of personal data where a data principal withdraws consent unless the retention is necessary for compliance with any other law. Rule 8(2) of the DPDP Rules also requires the data fiduciary to give the data principal notice 48 hours prior to the erasure of personal data. Imposing this obligation on citizens, researchers, whistleblowers, RTI activists, journalists, civil society organisations, and other stakeholders, would have wide-reaching implications, requiring them to even delete notes containing personal data. In the absence of a requirement to retain this personal data, journalists will be left with no option but to cease processing (which includes storage) and ultimately erase such personal data, making post-facto validation of a news report or article impossible. Moreover, if a data principal withdraws consent after the publication of a news story or article, merely because the opinion casts such data principal in doubtful light, journalists may be forced to takedown the article from their online websites. The absence of a public purpose exemption including for journalistic purposes from Section 12 of the DPDP Act threatens the freedom of speech and expression of journalists under Section 19(1)(a) of the Constitution of India.

KK. BECAUSE in the specific context of journalists like the Petitioners, the freedom of occupation of journalists is directly affected by the DPDP Act and the DPDP Rules, because processing personal data for public purposes including journalistic purposes is not exempted from complying with the obligations of data fiduciaries. Article 19(1)(g) of the Constitution of India protects the right to practise any profession or carry on any occupation, trade, or business. Journalists or persons undertaking journalistic activity invariably handle personal data in the course of carrying out their occupation, as

described above. These activities that lie at the heart of the occupation are unreasonably restricted by the DPDP Act, which imposes obligations upon them that are often impractical or infeasible or negate the very journalistic activity sought to be achieved through undertaking such processing, making the requirements under the DPDP Act violative of Article 19(1)(g) of the Constitution of India.

LL. BECAUSE the whole of the Impugned Act and the Impugned Rules is void for vagueness. As described above, several provisions of the Impugned Act and the Impugned Rules automatically apply to citizens, researchers, RTI activists, whistleblowers, on-ground reporters, civil society organisations, and other stakeholders who are collecting data in the public interest and to support journalistic activities of the Petitioners. Statutes can be void for vagueness because a statute that is precise will constitute adequate notice to persons on the applicability of the statute, and a non-vague law will not be applied in an arbitrary or non-discriminatory manner (*State of M.P. v. Baldeo Prasad, 1960 SCC OnLine SC 321*, [8-11]). The Impugned Act and the Impugned Rules are void for vagueness because they do not provide sufficient notice to the spectrum of persons to whom it becomes applicable, and who are not able to bear the onerous obligations of data fiduciaries, significant data fiduciaries, or the penalties that ensue from inadvertent non-compliance with such obligations.

MM. BECAUSE even though the DPDP Act has created a provision under Section 17(5) for exempting certain "data fiduciaries or class of data fiduciaries" from the provisions of the DPDP Act within five years from the date of commencement of the statute, the Central Government does not have the

power to exempt obligations of data fiduciaries in respect of a specific purpose, such as for public purposes, including for journalistic purposes.

III. SECTION 36 OF THE DPDP ACT READ WITH RULE 23 OF THE DPDP RULES EMPOWERING CENTRAL GOVERNMENT TO CALL FOR INFORMATION IS UNCONSTITUTIONAL AND VIOLATES ARTICLES 14, 19 AND 21 OF THE CONSTITUTION OF INDIA

NN. BECAUSE the protection provided by the DPDP Act for privacy is essential to human dignity and for the functioning of our democracy (*K.S. Puttaswamy I (supra)*, [297]). Section 36 of the DPDP Act states that the Central Government may require the Data Protection Board, any data fiduciary, or intermediary to provide information that it may call for. The Petitioners respectfully submit that Section 36 of the DPDP Act violates Articles 14, 19, and 21 of the Constitution of India. This provision authorises and facilitates unreasonable digital searches of personal data available with every data fiduciary or intermediary, contrary to Article 21 of the Constitution of India. Section 36 of the DPDP Act is vague, overbroad and arbitrary and the gathering and storage of personal information under this provision violates individual liberty and security of the person, contrary to Article 14 of the Constitution of India. To the extent that they prevent individuals from learning about disclosure of personal data to a government agency, they also infringe Article 19 of the Constitution of India. These infringements are not demonstrably justified in a free and democratic society.

OO. BECAUSE Section 36 of the DPDP Act enables government agencies to acquire personal data that is subject to a reasonable expectation of privacy without the consent of the individual whose information is sought, and then

allows the government to require the private organization to withhold the fact that the individual's information was requested.

PP. BECAUSE even though Section 36 of the DPDP Act does not state that rules may be prescribed under it, Rule 23(1) of the DPDP Rules requires data fiduciaries or intermediaries to furnish information pertaining to the purposes listed in Seventh Schedule of the DPDP Rules, within the specified period and through the corresponding authorised person. The purposes for which the Central Government may call for information are overbroad and vague, giving rise to the potential for abuse. The purposes are information (i) in the interest of sovereignty and integrity of India or security of the State; (ii) for the performance of any function under any law; (iii) for the disclosure of any information for fulfilling any obligation under any law; and (iv) for carrying out assessment for notifying any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary.

QQ. BECAUSE Section 36 of the DPDP Act read with Rule 23 of the DPDP Rules empowers the Central Government to call for information in the "interest of sovereignty and integrity of India or security of the State", a phrase that is both overbroad and vague, and is for that reason alone unconstitutional. A statute that suffers from overbreadth or vagueness is ripe for both constitutional and unconstitutional use by the State and its instrumentalities (*Shreya Singhal v. Union of India, (2015) 5 SCC 1,* [55-86]; *Chintamanrao v. State of M.P., 1950 SCC 695,* [13]; *State of Madras v. V.G. Row, (1952) 1 SCC 410,* [22-24]; *State of Bombay v. F.N. Balsara, 1951 SCC 860* [71-72]). To prevent arbitrary and discriminatory enforcement of a provision like Section 36 of the DPDP Act that allows the Central Government to call for information, laws must provide explicit standards for those who apply them.

This prevents impermissible delegation of basic policy matters to the State and its instrumentalities, which carries with it the dangers of arbitrary and discriminatory application. For this reason, Section 36 of the DPDP Act read with Rule 23 of the DPDP Rules is vague, overbroad and arbitrary contrary to Article 14 of the Constitution of India.

RR. BECAUSE in *PUCL* v. *Union of India*, (1997) 1 SCC 301 ["**PUCL**"], this Hon'ble Court in the context of a challenge to telephone tapping being challenged as a serious invasion of privacy, laid down certain steps and guidelines to be followed prior to interception. In *PUCL*, [28], this Hon'ble Court noted that Section 5(2) of the Telegraph Act, 1885 permits the interception of messages in circumstances mentioned therein i.e. "occurrence of any public emergency" or "in the interest of public safety". Second, the officer authorised by the Government had to be satisfied that it was "necessary or expedient" in the interest of five grounds enumerated under this section: (i) sovereignty and integrity of India; (ii) security of the State; (iii) friendly relations with foreign States; (iv) public order; or (v) preventing incitement to the commission of an offence. Moreover, the officer was empowered to issue the order for interception only after recording the reasons in writing. Another critical procedural safeguard outlined in the judgment was that the interception order, unless renewed, would cease to be effective after two months from the date of issue, and limited the total period of the operation of the order to six months. Detailed records were to be maintained of the intercepted communication and the procedure followed. The use of intercepted material was limited to the minimum necessary for the purposes under the Telegraph Act, 1885, and intercepted material would be destroyed when retention became unnecessary. Lastly, review committees were

expected to be constituted at Central and State levels to assess compliance with the law. These guidelines in PUCL were codified into law by Rule 419A of the Telegraph Rules, 1951. The Telecommunications Act, 2023 which repealed the Telegraph Act, 1885 also continues to maintain the safeguards in PUCL, through Rules 3, 4, and 5 of the Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 notified under Sections 20(2)(a) and 20(4) of the Telecommunications Act, 2023. The power to call for information under Section 36 of the DPDP Act from corporations and other entities that hold personal data is without any such procedural safeguards.

SS. BECAUSE Rule 23(2) read with Schedule VII of the DPDP Rules further stipulates that where the disclosure of such information is likely to "prejudicially affect the sovereignty and integrity of India or security of the State", the Data Fiduciary or the intermediary will be barred from disclosing that they have shared such information to the Data Principal who is affected, or to any other person unless they are permitted do so by relevant authorised person in writing. This would effectively mean that individuals whose personal data has been disclosed will only be made aware of the disclosure if either (1) they proactively seek out the information under the RTI Act *and* a public information officer does not block their request for information, or (2) if they face criminal charges. The DPDP Rules do not prescribe a procedure for the seeking the disclosure of data shared with the government pursuant to such requests. Such information disclosed to the government may have to be requested by the Data Principal by way of the RTI Act.

TT. BECAUSE this Hon'ble Court in *K.S. Puttaswamy I (supra),* [298, 307, 521, 525, 637] noted that for the purposes of the fundamental right to privacy,

meaningful and informed consent is required at every stage that the personal data is processed, used, or shared. Every instance of processing, using, or sharing personal data must be accompanied by consent. This refers to separate, discrete and individual instances of use after the initial consent was granted. Another supplementary safeguard besides consent is transparency and disclosure of the processing, using, or sharing of personal data.

UU. BECAUSE the privacy interest affected by government's requests for personal data is informational privacy, an interest squarely recognised in *K.S. Puttaswamy I (supra)*, [300, 301, 303, 521, 621, 629-636]. As the Supreme Court of Canada has noted in *R v. Bykovets, 2024 SCC 6,* [46] that, "[a]nonymity is a particularly important conception of privacy when it comes to the internet". Informational privacy protects the rights of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Given that the internet is increasingly integral to daily life, people should be able to reasonably expect that digital personal data generated by their activities and devices online will remain free from state searches and/or seizure.

VV. BECAUSE this Hon'ble Court noted in *K.S. Puttaswamy I (supra)*, [310], any intrusion to informational privacy will have to fulfill the three-part test of: (i) being prescribed by law; (ii) legitimate State aim; and (iii) proportionality of the action. Although the intrusion into the informational privacy of persons is established by way of a law, i.e. Section 36 of the DPDP Act, it authorises and facilitates unreasonable digital searches of personal data available with every data fiduciary or intermediary, contrary to Article 21 of the Constitution of India. First, Section 36 of the DPDP Act lacks the requirement for a specific independent authorization for the request of information. The judgment of this

Hon'ble Court in *K.S. Puttaswamy I (supra)*, [403], noted that Section 42 of the Narcotic Drugs and Psychotropic Substances Act, 1985 requires a specific authorization for search of a person even where there is suspicion. Meaningful oversight by way of a specific authorization to request for information performs an essential constitutional check on state intrusion into informational privacy of citizens. Second, Section 36 of the DPDP Act read with Rule 23 of the DPDP Rules contains no requirement to give notice to the data principal, if the information sought relates to the "sovereignty and integrity of India or security of the State". Indeed, individuals whose information has been shared with the Central Government pursuant to Section 36 of the DPDP Act, may never learn of the disclosure, unless it is revealed through subsequent criminal cases. Section 36 of the DPDP Act does not meet the minimum requirement of a data privacy regime conceived in *K.S. Puttaswamy I (supra)*, [298, 307, 521, 525, 637], where it was noted that every instance of processing or sharing personal data requires informed consent from the data principals.

WW. BECAUSE Section 36 of the DPDP Act read with Rule 23 of the DPDP Rules disproportionately empowers the Central Government to call for a broad category of information pertaining to information which is likely to "prejudicially affect the sovereignty and integrity of India or security of the State", without sufficient procedural safeguards. The Hon'ble Supreme Court struck down mandatory Aadhaar for phone SIMs on the basis that a dragnet collection of personal information without reasonable suspicion of specific wrongdoing was disproportionate (*K.S. Puttaswamy II*, [1453.2]); it also struck down parts of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and Rules therein, which for example, mandated too long a storage period for collected sensitive personal

data or information, or exhibited insufficient safeguards for the collection, processing, and use of data or information (*K.S. Puttaswamy II*, [1531-1549]). Section 36 of the DPDP Act read with Rule 23 of the DPDP Rules do not specify the retention period for data shared with the Central Government. The Central Government does not have to demonstrate a reasonable suspicion for collection of the data specified in Schedule VII of the DPDP Rules. Moreover, for information that can "prejudicially affect the sovereignty and integrity of India or security of the State", the Data Fiduciary or the intermediary is barred from disclosing that they have shared such information to the Data Principal who is affected, or to any other person unless they are permitted to do so by a relevant authorised person in writing, as specified in Schedule VII of the DPDP Rules.

XX. BECAUSE there is no limit to the kind of personal data that can be sought as necessary for the "sovereignty and integrity of India or security of the State". Personal data available with a variety of data fiduciaries may variously include, location history, contact networks, patterns of communication, which can reveal significant information about a person. It can be used to identify otherwise anonymous metadata obtained by various means, and it can also be used to identify anonymous online content obtained by various means. In doing so, it can identify and reveal intimate details about an individual's life—religious affiliations, political beliefs, sexual orientations, health concerns, or personal relationships. This limits or negatively impacts the liberty or security of that person. Moreover, as outlined above, the provision is unconstitutionally vague and does not provide meaningful guidance to prevent the risk of its unconstitutional application. It also lacks any oversight or accountability mechanism that independently authorizes the request for

information from the Central Government. As a result, Section 36 of the DPDP Act deprives and/or causes the risk of depriving an individual's liberty or security which is protected under Article 21 of the Constitution of India.

YY. BECAUSE the Central Government has a range of less intrusive alternatives, such as obtaining basic subscriber information with specific and independent authorisation from a court for a particular case, or limiting data collection to specific cases under judicial supervision. Without prejudice, the Central Government already enjoys a wide-range of search and seizure powers under various statutes, which inter-alia include, Section 94 (Summons to produce document or other thing), Section 105 (search without warrant) and Sections 185 (search with warrant) of the Bharatiya Nagarik Suraksha Sanhita, 2023. In fact, the recognition of a right to privacy in *K.S. Puttaswamy (I) (supra)*, should necessitate a critical review of the legality of search provisions under other statutes that are taken without procedural safeguards that can balance the right to privacy. Although Section 36 of the DPDP Act is not drafted in the nature of a provision authorising "searches", the underlying purpose for calling for information could be to undertake a search without the knowledge of the data principal. For this reason, the gathering and storage of personal information under Section 36 of the DPDP Act violates individual liberty and security of any person under Article 21 of the Constitution of India.

ZZ. BECAUSE Section 36 of the DPDP Act directly impacts the freedom of speech and expression of journalists by exposing journalists' private sources, whistleblowers, and informants to the potential for compromise of their personal identity and personal data. Preserving the confidentiality of sources is integral to investigative journalism, as journalists often rely on such informants for sensitive information. This Hon'ble Supreme Court in

Manohar Lal Sharma (Pegasus Spyware) v. Union of India, (2023) 11 SCC 401, [44-45] noted that an important and necessary corollary of a right to freedom of speech and expression of the press is to ensure the protection of journalistic sources. This Hon'ble Court noted that without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. The lack of a public purpose exemption for all citizens who wish to collect, process, and disseminate information for public purposes, including through journalistic expression, will likely deter potential informants from coming forward with necessary information for fear of their anonymity being compromised, thereby having a debilitating impact on robust journalism at large.

AAA. When information is requested by government agencies, without independent authorisation of such requests by a court order, it is effectively left to the government agencies to request for continued access to personal information. Data fiduciaries, for their part, will rarely have enough information to identify problematic requests from the Central Government, and would in fact proactively comply with such requests to avoid stringent penalties under the DPDP Act. In the particular context of journalists, civil society organisations, and citizens undertaking journalistic activities, who may be construed as a data fiduciary under the DPDP Act, Section 36 exposes private sources and whistleblowers who have shared critical information to journalists anonymously. The outcome of having a provision like Section 36 of the DPDP Act is a legislative framework that permits government access to personal information without accountability mechanisms, reasoning, judicial oversight, or transparency, violating the constitutional rights recognised in Articles 14, 19, and 21 of the Constitution of India.

IV. THE DATA PROTECTION BOARD LACKS INDEPENDENCE AND RESTRICTS FREEDOM OF SPEECH AND EXPRESSION

BBB. BECAUSE this Hon'ble Court in *K.S. Puttaswamy II (supra)*, considered the principles laid down in *K.S. Puttaswamy I (supra)* when considering the constitutionality of the Aadhaar programme and the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. In the context of potential personal data violations arising from the Aadhaar programme, this Hon'ble Court noted that an independent regulatory framework is required for a strong regime of data protection.

CCC. BECAUSE this Hon'ble Court in *K.S. Puttaswamy II, [1355],* specifically, in the context of the UIDAI, this Hon'ble Court noted that it is established and controlled by the Central Government, and possesses neither the autonomy nor the regulatory authority to enforce the mandate of the law in regard to the protection of data.

DDD. BECAUSE the DPDP Act establishes the Data Protection Board ("**DPB**"), and under Section 28(1) of the DPDP Act states that the DPB will purportedly function as an "independent" body. Under Rules 17(1) of the DPDP Rules, 3 Secretaries of the Central government and 2 experts nominated by the Central Government are tasked with the constitution of a Search-cum-Selection Committee to recommend individuals for appointment as Chairperson. Under Rule 17(2) of the DPDP Rules, 2 Secretaries of the Central Government and 2 experts nominated by the Central Government are tasked with the constitution of a Search-cum-Selection Committee to recommend individuals for appointment as members to the DPB. Rule 17(3) of the DPDP Rules states that the Central Government shall appoint the Chairperson or other Member, after considering the suitability of individuals recommended by the Search-

cum-Selection Committee. This does not mandate that the Central Government appoint the Chairperson or other Member from the list of persons recommended by the Search-cum-Selection Committee. Thus, under the present legal framework, the authority to finalise the appointments to the DPB rests with the Central government. The DPB, is the designated body to adjudicate complaints and impose penalties under the DPDP Act. The DPB's process of appointing its Chairperson and members raises concerns of executive control and questions regarding its independence and impartiality. Given that the State, its agencies and the public sector are the largest data fiduciaries and processors, the DPB's appointments process raises an apprehension regarding the independence of the DPB, as the process could be influenced by political considerations, undermining the DPB's credibility and impartiality.

EEE. BECAUSE the Central Government cannot simply override or contradict the judicial decisions of this Hon'ble Court by re-enacting or repackaging the same form of law in a different form (*Madras Bar Assn. v. Union of India, 2025 SCC OnLine SC 2498 ("***MBA 2025***")*, [140, 141, 149]). In a series of cases prior to *MBA 2025*, where the constitutionality of tribunals comprised of members appointed by the Executive exercising powers equivalent to constitutional courts was in question, this Hon'ble Court has insisted that "independence, impartiality, and effective adjudication" of tribunals strike at the core of the constitutional arrangement of separation of powers and judicial independence (*Madras Bar Assn. v. Union of India, (2022) 12 SCC 455 ("**MBA 2021**")*, [55-66]; *Madras Bar Assn. v. Union of India, (2021) 7 SCC 369 ("**MBA 2020**")*, [35, 40, 60]; *Rojer Mathew v. South Indian Bank Ltd.,*

(2020) 6 SCC 1, [149, 154]; *Union of India v. Madras Bar Assn., (2010) 11 SCC 1*, [90]; *L. Chandra Kumar v. Union of India, (1997) 3 SCC 261*, [78]).

FFF. BECAUSE provisions of the DPDP Act pertaining to the DPB were notified on 13.11.2025. These provisions continue to have issues concerning independence and impartiality. When the Parliament passed the Tribunal Reforms Act, 2021, this Court in MBA 2025 noted that it was "substantively identical" to the Tribunal Reforms Ordinance, 2021. This Hon'ble Court in *MBA 2021* struck down those provisions of the Tribunal Reforms Ordinance, 2021, which did not conform to the requirements of the directions given in *MBA 2020*, with Justice Nageswara Rao in *MBA 2021*, [56] describing these departures from the *MBA 2020* regime as an "impermissible legislative override". Further, in *MBA 2025*, [123] this Hon'ble Court noted that its directions with respect to constitutional principles such as those concerning independence, composition, or tenure of adjudicatory bodies are mandatory and binding. This Hon'ble Court in *MBA 2025*, [116] noted that when it strikes down a provision or has issued binding directions after identifying a constitutional defect, Parliament "cannot simply override or contradict that judicial decision by reenacting the very same measure in a different form." In other words, the Parliament may "cure" defects identified by this Hon'ble Court but cannot simply "restate or repackage" what has been struck down.

GGG. BECAUSE from the purview of journalists, civil society organisations, and citizens who pursue journalistic activities, it is of great concern that their ability to freely report news stories would depend on the adjudication of mere complaints to the DPB under the DPDP Act for non-compliance with the onerous obligations which may attract unaffordable and stringent penalties.

HHH. BECAUSE the functioning of the DPB as a digital office will make it exclusionary and outside the reach of many citizens who are not adept at using technology even though their digitized personal data is governed by the DPDP Act. Section 28(1) of the DPDP Act states that the DPB shall function as a "digital office" with the receipt of complaints and the allocation, hearing, and pronouncement of decisions being "digital by design".

III. BECAUSE the penalties prescribed in the Schedule to the DPDP Act in respect of data fiduciaries range from Rs. 50 Crore to Rs. 250 Crores. The penalties indicated in the DPDP Act are exaggerated and do not reflect the various kinds of individuals and entities who are likely to be classified as data fiduciaries. This penalty regime dissuades journalists from news reporting, given that a minor and inadvertent transgression leaves them exposed to unaffordable penalties.

JJJ. BECAUSE Section 33(2) of the DPDP Act states that the relevant factors to be considered while imposing penalties include, the (i) nature, gravity and duration of the breach and (ii) likely impact of the imposition of the monetary penalty on the person. The inclusion of these factors reflects the understanding that a variety of individuals and organisations are likely to be covered within the scope of the DPDP Act as data fiduciaries. However, it is important to recognize that journalists, media, and citizens who pursue journalistic activities, are likely part of the class of data fiduciaries who cannot afford to pay the penalties prescribed by the Schedule to the DPDP Act.

KKK. BECAUSE even though the DPDP Act has created a provision under Section 17(5) for exempting certain "data fiduciaries or class of data fiduciaries" from the provisions of the DPDP Act within five years from the date of commencement of the statute, the Central Government does not have the

power to exempt obligations of data fiduciaries in respect of a specific purpose, such as for public purposes, including for journalistic purposes.

LLL. BECAUSE for all the above reasons, the Data Protection Board lacks independence and restricts freedom of speech and expression by its punitive penalty regime.

59. The Petitioners have not filed any such similar petition challenging the Impugned Act or the Impugned Rules in this Hon'ble Court or in any other High Court or courts below.

PRAYER

Therefore, in light of the above-mentioned facts and circumstances, it is respectfully prayed that this Hon'ble Court may kindly be pleased to:

A. Issue a writ in the nature of *mandamus*, or any other appropriate writ, order, or direction declaring the whole of the Digital Personal Data Protection Act, 2023, and specifically Sections 5, 6, 8, 10, 17, 18, 19, 36, and 44(3), of the Digital Personal Data Protection Act, 2023, to be void, inoperative and unconstitutional for being ultra vires Articles 14, 19, and 21 of the Constitution;

B. Issue a writ in the nature of *mandamus*, or any other appropriate writ, order, or direction declaring the whole of the Digital Personal Data Protection Rules, 2025, specifically Rules 3, 6, 7, 8, 9, 13, 16, 17, and 23 of the Digital Personal Data Protection Rules, 2025, to be void, inoperative and unconstitutional for being ultra vires Articles 14, 19, and 21 of the Constitution;

C. Issue any other writ, order or direction as this Hon'ble Court may deem fit and proper to do complete justice in the circumstances of the case.

AND FOR THIS ACT OF KINDNESS THE PETITIONERS AS IS IN DUTY BOUND SHALL REMAIN EVER GRATEFUL.

DRAWN BY:

1. Mr. Apar Gupta, Adv.
2. Mr. Muhammad Ali Khan, Adv.
3. Ms. Indumugi C., Adv.
4. Mr. Naman Kumar, Adv.

FILED BY:

Date: 13.02.2026
Place: New Delhi

ABISHEK JEBARAJ
Advocate for the
Petitioners

IN THE SUPREME COURT OF INDIA

(CIVIL ORIGINAL JURISDICTION)

WRIT PETITION (CIVIL) NO. OF 2026

(Under Article 32 of the Constitution of India)

IN THE MATTER OF:

The Reporters' Collective Trust & Anr. ...Petitioner

versus

Union of India & Ors. ...Respondents

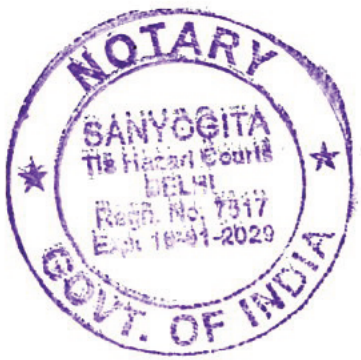
AFFIDAVITS

I, Mayank Aggarwal, authorised representative of the Reporters' Collective Trust Petitioner No. 1, having office at 1/22, Asif Ali Road, New Delhi - 110002, presently at New Delhi. Do hereby solemnly affirm and state on oath as follows:

1. That I am authorised representative of the Reporters' Collective Trust, Petitioner No. 1 and am fully aware of the facts and circumstances surrounding the present case. Thus, I am competent to swear and depose the present affidavit on behalf of the Petitioner.

2. That I am conversant with the facts and circumstances of the case and am competent to swear this affidavit.

3. That I have read the contents of the accompanying Synopsis and list of dates (page B to Q), Writ Petition(page 1 to 80) and IAs (page no. 272 to 279) and state that the same are true to the best of my knowledge. information and belief.



4. That the instant petition is based on information available in the public domain. That the Annexures are true to their respective originals.

5. That I have done whatever inquiry/investigation that was in my power to do and collect all data/material which was available and which was relevant for this court to entertain the present writ petition. I further confirm that I have not concealed in the present writ petition any data/material/information which may have enabled this Hon'ble Court to form an opinion whether to entertain the present writ petition or not and/or whether to grant any relief.

6. That there is no personal interest/gain, private motive or oblique reason in filling the present writ petition.

For The Reporters Collective Trust

Trustee

DEPONENT

VERIFICATION

I do hereby verify that the contents of the above affidavit are true and correct to the best of my knowledge and no part of it is false and that nothing material has been concealed therefrom.

Verified at New Delhi on this day of of 2026

For The Reporters Collective Trust

Trustee

DEPONENT

ATTESTED

NOTARY PUBLIC DELHI

NOTARY SANYOGITA Tis Hazari Courts DELHI Regn. No. 7517 Exp. 10-01-2029 GOVT. OF INDIA

11 FEB 2026

IN THE SUPREME COURT OF INDIA

(CIVIL ORIGINAL JURISDICTION)

WRIT PETITION (CIVIL) NO. OF 2026

(Under Article 32 of the Constitution of India)

IN THE MATTER OF:

The Reporters' Collective Trust & Anr. ...Petitioner

versus

Union of India & Ors. ...Respondents

AFFIDAVITS

I, Nitin Sethi S/o K L Sethi Aged 51 [redacted] presently at New Delhi. Do hereby solemnly affirm and state on oath as follows:

1. That I am the Petitioner No. 2 and am fully aware of the facts and circumstances surrounding the present case. Thus, I am competent to swear and depose the present affidavit on behalf of the Petitioner.

2. That I am conversant with the facts and circumstances of the case and am competent to swear this affidavit.

3. That I have read the contents of the accompanying Synopsis and list of dates (page B to Q), Writ Petition(page 1 to 80) and IAs (page no. 272 to 279) and state that the same are true to the best of my knowledge. information and belief.

4. That the instant petition is based on information available in the public domain. That the Annexures are true to their respective originals.

5. That I have done whatever inquiry/investigation that was in my power to do and collect all data/material which was available and which was relevant for this court to entertain the present writ petition. I further confirm that I have not concealed in the present writ petition any data/material/information which may have enabled this Hon'ble Court to form an opinion whether to entertain the present writ petition or not and/or whether to grant any relief.

6. That there is no personal interest/gain, private motive or oblique reason in filling the present writ petition.

DEPONENT

VERIFICATION

I do hereby verify that the contents of the above affidavit are true and correct to the best of my knowledge and no part of it is false and that nothing material has been concealed therefrom.

Verified at New Delhi on this day of of 2026

DEPONENT

ATTESTED

NOTARY PUBLIC DELHI

NOTARY SANYOGITA Tis Hazari Courts DELHI Regn. No. 7517 Exp. 10-01-2029 GOVT. OF INDIA

11 FEB 2026