THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

May 28, 2025

Challenge of Balancing Privacy and Transparency

By: Prashant Reddy T

With the right to privacy guaranteed in India, the state cannot force public disclosure of personal data. Access must be justified on the ground of legitimate interests, empowering bureaucrats to decide. This clashes with the RTI Act, which traditionally granted access without requiring reasons.

Over the past few months, transparency activists have launched an advocacy campaign to oppose an amendment to the Right to Information Act, 2005 (RTI). This amendment was brought in via the Digital Personal Data Protection Act, 2023 (DPDP), which modified Section 8(1)(j) of the RTI Act. At its core, this debate is about balancing the fundamental right to privacy with the right to information, which is also a fundamental right in India. The tension between the right to privacy over information and the right to access information is difficult to navigate since these values are fundamentally opposed to each other.

As originally enacted, Section 8(1)(j) allowed the state to deny requests for "personal information" that had no connection to public activity or would cause an unwarranted invasion of the privacy of the individual, except in cases where the "larger public interest justified the disclosure of such information."

This was a poorly drafted provision because it was written in a circular manner – private was what was not public. The amendment brought in by the DPDP Act has now deleted the "public activity" and "public interest" exemptions in Section 8(1)(j), thereby introducing a blanket ban on the disclosure of all "personal information" in government records.

Origins of right to privacy

The government has justified the amendment on the grounds that it was necessitated by the 2017 judgment of the Supreme Court in the *Puttaswamy case*, which declared privacy to be a fundamental right. Contrary to its critics, there is some merit to this argument. A good starting point is to understand the origins of the theory of "informational self-determination," which was at the centre of the right to privacy campaign that resulted in the *Puttaswamy* judgment. This theory had its origins in Nazi Germany, where census information was allegedly processed by IBM machines to identify Jews and other minorities who were later killed in concentration camps.

> The European approach to privacy has made it very difficult to maintain publicly accessible databases where the state proactively discloses information in the interests of transparency.

Postwar West Germany was therefore very sensitive about the manner in which the state could store and process the personal data of citizens to create profiles of individual citizens by accessing and linking multiple databases. For example, if bureaucrats could access a citizen's census data along with his or her tax information, land ownership record, health data, and police record, they could theoretically create a complete profile of the person. This access would give them enormous power over individual citizens.

It was such an argument that formed the basis of a landmark judgment of the highest constitutional court in Germany – the Bundesverfassungsgericht – in 1983, when it recognised the citizen's right to "informational self-determination." The case involved the manner in which the German state was collecting personal data for the census and processing it using modern data processing technologies. The chief concern was the ability of the state to use the personal data to build personal profiles of individual citizens by supplementing it with information from other databases maintained by it. The German court ruled against such practices, stressing the need to balance the state's right to collect statistical data with the right of citizens to control the use of their personal data. The principles laid down in that case gradually evolved to become the foundation of the privacy framework of the European Union.

In practice, this European approach to privacy has made it very difficult to maintain publicly accessible databases where the state proactively discloses information in the interests of transparency. Two examples will help drive home the point of the damage caused to transparency in public governance because of the European approach to privacy.

The first was the scrubbing of all personal data on the WHOIS public database in 2018 because of Europe's new privacy law. This database contained crucial ownership details of all websites on the internet. Without this database, it has become very difficult to access

information on ownership of websites, making the internet a less accountable, more dangerous place. As of today, anybody can register a publicly accessible database to slander an individual while hiding behind a veil of secrecy. In theory, it should be possible to get a court order to unmask the individual but this would be a very expensive process and reasons must be provided to convince a judge that disclosure is necessary. Compared to this, the original WHOIS, which required all websites to publicly reveal their ownership data, was much simpler and promoted greater transparency.

The second example is from 2022 when the European Court of Justice (ECJ) declared public registers of beneficial ownership to be violative of the privacy and personal data protection clauses in the Charter of Fundamental Rights of the European Union. Transparency International sharply criticised the ECJ's judgment because the public registers made it possible to identify the people who own or control companies, making it easier to track the flow of illicit money. The ECJ, however, looked at the issue differently. It ruled that citizens' privacy could not be sacrificed simply for the state's goal of tracking illegal funds. The state may investigate such funds, but only if it can show sufficient reason to override the default right to privacy regarding beneficial ownership. Such an interpretation of privacy puts an end to the concept of public registers that display personal information to the entire world.

Clash with transparency

Returning to the amendment to Section 8(1)(j), it was but logical that the "public interest" exception had to be deleted after the *Puttaswamy* judgment declared privacy to be a fundamental right. Fundamental rights by their very definition are meant to protect the individual against the state. Any exceptions to fundamental rights are typically narrow. Take, for example, Article 19(2) of the Constitution, which lists out nine grounds that can form the basis of reasonable restrictions on the fundamental rights to free speech, trade, and so on. There is no broadly worded "public interest" clause in Article 19(2).

> Fundamental rights by their very definition are meant to protect the individual against the state. Any exceptions to fundamental rights are typically narrow.

Similarly, in the context of personal information in public records, once the court declared privacy to be a fundamental right, it followed that any exception had to be limited and narrow. A broad-based "public interest" exception, as in Section 8(1)(j) of the RTI Act, is neither narrow nor limited. In effect, a public interest exception allows the state to overrule an individual's fundamental right in the larger public interest. There is no doubt that the "public interest" exception had to go after the judgment in *Puttaswamy*.

One could argue that Parliament should have winnowed down the "public interest" exception in Section 8(1)(j) in line with the Supreme Court conclusion in the *Puttaswamy* case that the right to privacy could be curbed to meet the "legitimate interests" of the state. Illustratively, the court identified the "legitimate interests" of the state as protecting national security, preventing crime, and preventing the dissipation of social welfare benefits. At no point did it advocate for a broad "public interest" exception to the fundamental right to privacy.

Challenges to public databases

A far bigger concern for transparency campaigners in the future will be the inevitable constitutional challenges to the many public databases that have helped boost public confidence in public administration and electoral politics. Take, for example, the Jan Soochna Portal in Rajasthan. This is a digital version of the "transparency walls" pioneered in the state, which made information on all beneficiaries of schemes in villages, including their addresses, available to the public. The walls displaying the information helped villagers conducts "social audits" by verifying recipients of benefits thereby ensuring that bureaucrats did not siphon away benefits such as essential rations to "ghost beneficiaries". The Jan Soochna Portal replicated this approach in the digital space for all districts of Rajasthan. Anyone can identify beneficiaries of welfare programmes in Rajasthan with a few mouse clicks.

Apart from this, many e-governance programmes across the country related to land records or voter lists are premised on the same model of proactive disclosure of personal information to the general public. These public databases are now technically violative of a citizen's right to privacy because once the law recognises the right of citizens to control their access to information, the state cannot force them to proactively disclose such information to the general public.

> In the Indian context, this would largely upend the scheme of the RTI Act, which was meant to provide citizens with information without them having to provide reasons for why they wanted it.

Such personal information can still be accessed, but only by the state and only when the legitimate interests of the state are involved. This necessarily means giving a bureaucrat the power to decide whether the reason to access the information is legitimate according to the law. In the Indian context, this would largely upend the scheme of the RTI Act, which was meant to provide citizens with information without them having to provide reasons for why they wanted it. To this extent, a definition of privacy grounded in the European theory of informational self-determination is fundamentally opposed to transparency through proactive disclosures. These are opposing values, which can never be reconciled.

The *Puttaswamy* judgment also has the potential to undo the 2002 decision of the Supreme Court, which forced the political class to disclose their assets, educational qualifications, and criminal records before elections. That decision of the court paid little attention to the issue of privacy because it was not a fundamental right in 2002. After *Puttaswamy*, politicians and their families, who enjoy fundamental rights like any other citizen, can argue that they cannot be compelled to disclose personal information on the mere assumption that all of them are corrupt. Instead, they could argue that it should be voluntary to disclose assets and personal wealth and that the state can access such information only for a criminal investigation. Such an argument would resonate loudly with judges of the Supreme Court who could use a similar argument to not disclose their own assets to the public.

If the courts step in to declare public databases unconstitutional, there is little that Parliament can do to remedy the situation. This is because the Supreme Court is the ultimate arbiter of fundamental rights. Once privacy was declared as a fundamental right by the Supreme Court, the balance of power shifted away from Parliament in favour of the courts.

In the context of transparency, this is not necessarily good news because the track record of courts with regard to enabling transparency in public administration has not been encouraging. For instance, in the *Girish Deshpande* case, the Supreme Court declared that the service records of bureaucrats, including their disciplinary records, could not be disclosed under the RTI Act as it would be violative of their right to privacy. For the most part, the judiciary has not been welcoming of the RTI Act and the institution continues to operate behind a veil of secrecy. There is little that democratic power can do to change these judicial attitudes because the court has been designed to resist majoritarian pressure.

Need for meaningful debate

It is now too late to undo the *Puttaswamy* judgment or the amendment to Section 8(1)(j) of the RTI Act. It is, however, important to understand and acknowledge that the demand for declaring privacy as a fundamental right, in terms of the European notion of informational self-determination, came from within civil society and not the state. It was a ferocious civil society campaign against the Aadhaar identification program that resulted in privacy being declared a fundamental right. The state actually opposed privacy being declared a fundamental right. These are important facts that are conveniently forgotten during public debates in India over privacy and transparency.

> It is […] important to understand and acknowledge that the demand for declaring privacy as a fundamental right, in terms of the European notion of informational self-determination, came from within civil society and not the state.

Each side of the debate keeps quiet while the other side publicly demands stronger privacy or transparency rights. When anti-Aadhaar activists sought stronger privacy rights, none of the transparency activists spoke up. Now that the transparency activists are opposing the amendment to the privacy clause in the RTI Act, nobody from the privacy camp is speaking up. These issues are seldom discussed in public, preventing Indians from engaging in a more informed and meaningful debate.

Prashant Reddy T. has been a user of the Right to Information Act for the last 15 years and is co-author of Create, Copy, Disrupt: India's Intellectual Property Dilemma *(Oxford University Press: 2017).*