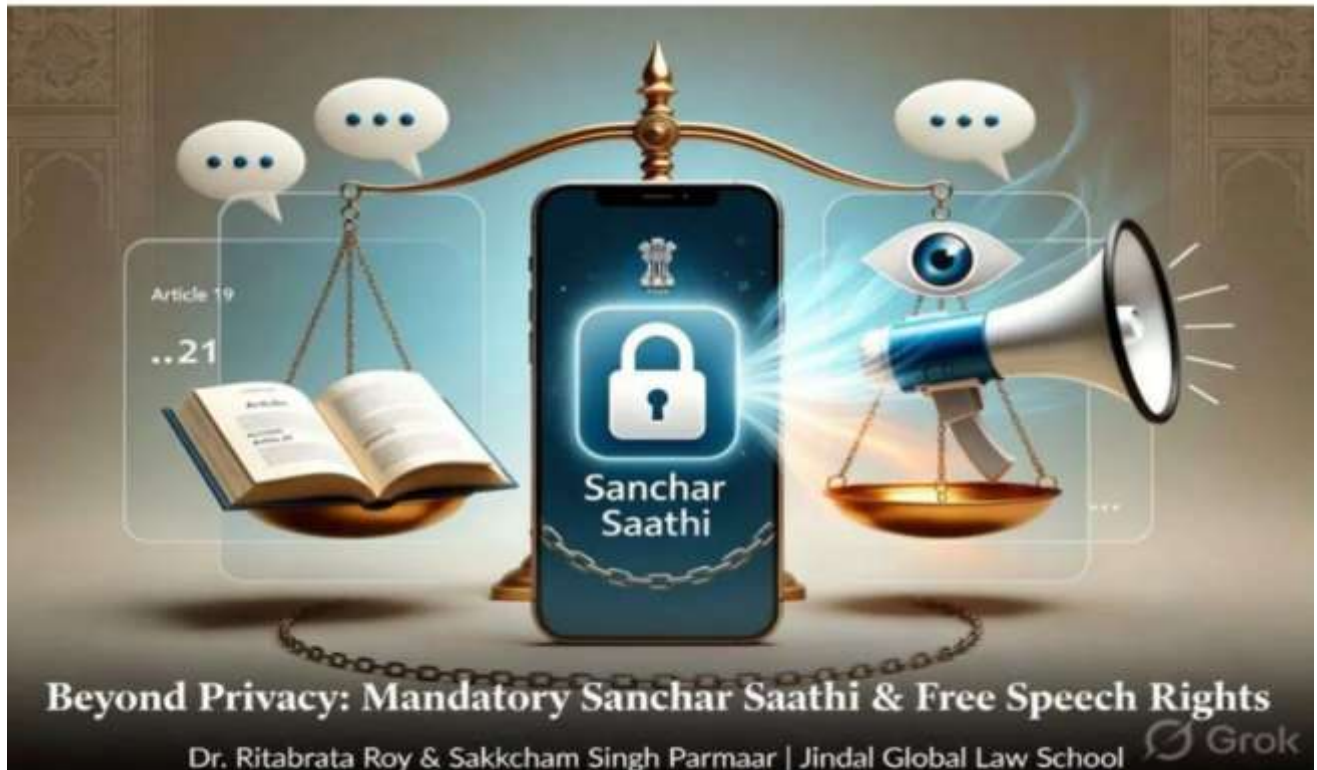


Beyond Privacy: Mandatory Sanchar Saathi & Free Speech Rights

As India marches further into the digital age, we call for voluntary participation, informed consent, and unwavering respect for fundamental rights in all future digital governance initiatives.

Sartaj Singh
04 Aug 2026



New Delhi, July 31, 2026

When the Department of Telecommunications proposed making the Sanchar Saathi app pre-installed and non-removable on all smartphones, the public outcry centred almost exclusively on privacy and data protection. But according to a new constitutional analysis by legal scholars from Jindal Global Law School, that debate missed the far more fundamental constitutional violation lurking beneath the surface.

In our analysis, we argue that the mandate was not merely a privacy infringement under Article 21 but an unprecedented and direct assault on freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India.

The government has since withdrawn the mandatory provision, but the constitutional questions it raised remain unanswered and urgently relevant for future digital governance initiatives.

A New Kind of Restriction: Structural, Not Content-Based

Traditional restrictions on free speech such as those listed under Article 19(2) are reactive in nature. The state identifies harmful content obscenity, defamation, threats to public order and regulates it after it has been expressed. These are content-based limitations that target the substance of what is said.

The Sanchar Saathi mandate, however, operated entirely differently. It did not regulate speech based on its content. Instead, it sought to alter the very architecture of communication before any speech could even occur.

By compelling every smartphone to permanently host a state-prescribed application, the state transforms a privately owned medium of communication into a state-architected space. This, we argue, constitutes a "structural" or "architectural" restriction a form of prior restraint that Indian courts have historically viewed with the "heaviest presumption" against its constitutionality.

The Chilling Effect on Democratic Discourse

Perhaps the most alarming consequence of the mandate, according to our analysis, was the chilling effect it would have inevitably produced on democratic expression.

The knowledge that a non-removable state application with access to communications metadata such as call logs, SMS headers, and device identity was permanently installed on their smartphones would have discouraged citizens from engaging in sensitive political discourse, communicating with journalists, or exercising their right to lawful dissent.

The compulsion here is not about what you say, but about the space in which you say it. That space ceases to be private the moment the state permanently occupies it. We warn that this would have stifled the "free trade of ideas" that Article 19(1)(a) is fundamentally designed to protect.

Failing the Puttaswamy Proportionality Test

A significant portion of our analysis applies the proportionality framework established by the Supreme Court in the landmark *K.S. Puttaswamy v. Union of India* judgment. Any state action that interferes with a fundamental right must satisfy a three-part test: it must be (i) prescribed by law, (ii) pursue a legitimate state aim, and (iii) be proportionate to that aim.

We acknowledge that preventing telecom fraud and enhancing digital communication security are legitimate state interests. However, we strongly question whether the mandatory installation requirement passed the proportionality threshold.

The state has not substantiated why less intrusive and rights-respecting alternatives would not serve its legitimate aims. We point to a simple alternative: a voluntary opt-in model combined with a public awareness campaign. Such an approach would achieve the same security objectives without compelling every citizen to permanently alter their personal device.

We further contend that the mandate imposed a grossly disproportionate burden affecting over one billion mobile phone users, most of whom are not fraudsters for a benefit aimed at addressing a relatively narrow harm. Weighing the purported security benefits against the far-reaching prevention of expressive liberty being imposed upon citizens creates an imbalance.

In Conflict with the Digital Personal Data Protection Act, 2023

Beyond constitutional free speech concerns, our analysis also interrogates the mandate through the lens of India's Digital Personal Data Protection Act (DPDPA), 2023.

The DPDPA is built on the foundational principle of free, specific, informed, unconditional, and revocable consent. We argue that forcing software onto a personal device pre-installed and non-removable is fundamentally irreconcilable with this framework.

Consent granted under coercion whereby the user's device is presented with the app pre-loaded and is non-removable is not free. We also raise concerns about "function creep" the risk that a permanently installed application, initially justified for anti-fraud purposes, could over time acquire additional functions or responsibilities. This could expand state surveillance capacities far beyond the original intent, chilling expression without adequate legislative oversight.

Constitutional Precedent: The Right to Silence

We draw on a crucial constitutional precedent: the Supreme Court's ruling in *Bijoe Emmanuel v. State of Kerala*, which held that freedom of speech under Article 19(1)(a) also includes the right to silence the right not to be compelled to express a sentiment against one's will.

We extend this principle to the digital realm. The Sanchar Saathi mandate did not compel citizens to speak but it compelled them to make their personal communication devices permanently available for a state-prescribed function. In an age where smartphones are extensions of an individual's personal and mental space, this compulsion is the 21st-century equivalent of forcing a citizen to display a state symbol on their private property.

A Dangerous Precedent

We also place the Sanchar Saathi proposal in the broader context of India's digital policy trajectory, drawing comparisons with the evolution of Aadhaar which began as a voluntary scheme but gradually became compulsory.

The universal compulsory pre-installation of state software on personal devices is the hallmark of authoritarian surveillance regimes. In open democratic systems, security tools are offered on a voluntary, consent-based basis precisely to sustain the integrity of the private sphere. The Sanchar Saathi mandate would have eroded that critical normative space.

Conclusion: A Narrow Escape

The government's decision to withdraw the mandatory provision is welcome but it must be seen as more than just a policy rethink. It was a narrow escape from a monumental constitutional crisis.

The potential hazard was not just an infringement of privacy, but a direct attack on the architecture of free speech guaranteed under Article 19(1)(a). By attempting to attach a state application onto the primary device of modern communication as a permanent fixture, the government sought to impose a form of structural pre-emptive restraint that would have failed the Puttaswamy proportionality test and contravened the consent-based core of the DPDPA.

As India marches further into the digital age, we call for voluntary participation, informed consent, and unwavering respect for fundamental rights in all future digital governance initiatives. The smartphone must remain a space of private speech and personal freedom not an instrument of state control.

About the Authors:

1) Dr. Ritabrata Roy is Assistant Professor at Jindal Global Law School, O.P. Jindal Global University.

2) Sakkcham Singh Parmaar is a BA LLB (Hons.) student at Jindal Global Law School, O.P. Jindal Global University.