VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

PRIVACY AND DATA PROTECTION POST-PUTTASWAMY JUDGMENT: LEGAL GAPS, EMERGING TECHNOLOGY, AND THE INDIAN LANDSCAPE

- Amaan Tamboli*

Abstract

Back in 2017, the Supreme Court's ruling in Justice K.S. Puttaswamy v. Union of India felt like a real shift in Indian constitutional law. Suddenly, privacy wasn't just a nice idea—it was a right, woven into the fabric of life, liberty, and dignity under Article 21. The judges didn't just stop at abstract principles; they put informational self-determination at the heart of what it means to control your own life, especially in a world run by digital systems, relentless data collection, and platform-based interactions.

But jump ahead almost a decade, and the reality looks quite different. There's a constant gap between what the Constitution promises and how the system actually works. Post-Puttaswamy, India still runs a data ecosystem that cares more about surveillance, traceability, and making things easy for administrators than it does about privacy-by-design.

Look closely at the legal and technical landscape. The Digital Personal Data Protection Act, 2023, Aadhaar-based identity systems, UPI payments, and government-mandated apps like Sanchar Saathi—these aren't just isolated examples. They reveal the bigger picture: weak independent oversight, sweeping state exemptions, and no real proportionality analysis when it comes to digital schemes. The state keeps expanding its reach while independent checks remain flimsy at best.

Now, contrast this with privacy-preserving technologies elsewhere. Take Apple Pay's tokenization, for instance—it shows that privacy-first systems aren't just a pipe dream. They're

*Student at Maharashtra National Law University, Chh. Sambhajinagar (Aurangabad)

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
https://www.ijalr.in/

possible, and they work. India's insistence on traceability isn't technically inevitable; it's a choice. The Constitution demands more.

So, what's next? To actually fulfil the promise of Puttaswamy, reforms need to go beyond words. That means building strong, independent institutions, embedding privacy-by-design into every digital system, and making sure courts have teeth when it comes to oversight. Only then does privacy become a living, breathing part of India's digital future—not just a line in a judgment.

INTRODUCTION

Justice K.S. Puttaswamy v. Union of India [1]wasn't just theory. The Court looked straight at the reality of India speeding into the digital age—identity databases, fintech, social media, algorithms making decisions nobody voted for. The judges warned that if we let data collection run wild, it threatens the core of constitutional democracy. To check that power, they set up a clear three-part test for when the State wants to intrude on privacy: the law must authorize it, the goal must be legitimate, and the measure must be proportionate. In plain terms, the government has to show its methods make sense, that they're necessary, and that there's no less intrusive way to get the job done.

Yet, even after this landmark ruling, India's digital growth since 2017 has mostly focused on traceability, security, and making administration smoother. Data minimization, anonymization, and actual user control? These often get sidelined. From Aadhaar-based welfare to UPI payment footprints to surveillance-driven "cyber-safety" tools, people now live inside systems that track them constantly, in detail, and mostly out of sight. This article digs into how the law responds to that reality.

THE POST-PUTTASWAMY LEGAL FRAMEWORK

A. The Digital Personal Data Protection Act, 2023

India's Digital Personal Data Protection Act, 2023 is the country's first real attempt to rein in how digital personal data gets handled. It brings in ideas like "data fiduciaries" (those who handle data) and "data principals" (the people the data is about). The Act talks about consent,

[1]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 168–169 (India)

clear limits on why data gets used, asking only for what's needed, keeping data secure, and telling people when a breach happens. In theory, it lines up with the privacy rights the Constitution promises—notice, consent, the right to take back consent, and a way to complain if your data's misused.

But if you look closer, this law steps away from the proportionality standard the Supreme Court set out in the Puttaswamy case. It creates broad "legitimate use" categories where the government (and others) can process data without asking for consent. Say you're applying for a government benefit or license—the State can process your data without your say-so. These exceptions weaken the idea that data should only be used for specific purposes, and make consent feel almost meaningless in the public sector. Worse, the central government keeps the power to exempt whole groups—entire departments or types of data handlers—from the law's main rules.

Then there's the Data Protection Board the Act sets up. On paper, it's supposed to keep an eye on how the rules are followed. In reality, its members and leadership are chosen by the executive, which means it's not really independent. If the government is overreaching, can this Board stand up to it? That looks doubtful. In the end, the DPDP Act risks turning state surveillance into a permanent feature, all while pretending to protect privacy. Instead of letting people control their own information, it hands the State a blank check to collect and use personal data.

B. Surveillance Frameworks and the Sanchar Saathi App

India's surveillance system still leans on old laws like the Telegraph Act and the Information Technology Act, 2000. These laws, along with a tangle of executive rules and sector-specific regulations, let the government intercept, monitor, and even decrypt communications, all in the name of national security or public order. But here's the thing—they were written before the Supreme Court's Puttaswamy judgment, and they mostly hand power to the executive, shutting out real judicial oversight from the start.

Take the Sanchar Saathi app as a case in point. Authorities wanted it pre-installed on every smartphone, and at first, you couldn't even delete or disable it. That set off immediate alarm

bells among digital rights groups. Even after officials walked it back and called the app "optional," reports surfaced showing it still grabs sensitive data—phone numbers, call logs, SMS details—all under the banner of fighting fraud and blocking stolen devices.

When you look at this through the lens of the current DPDP regime, which gives the state sweeping exemptions, Sanchar Saathi makes three big problems obvious. First, there's no real remedy if you're tracked without cause. Second, it's unclear who's responsible when the government pushes out this kind of software. Third, independent oversight is almost nonexistent. The app shows just how easily privacy can get swept aside in the name of public interest, all without any real proportionality check or meaningful debate.

C. Aadhaar–Bank–Mobile Linkages

Aadhaar now sits at the center of India's welfare and financial systems. It ties people's biometric identities to their bank accounts, phone numbers, and payment platforms. Even though the Supreme Court blocked mandatory Aadhaar in some private settings, on the ground, people still feel forced to link their Aadhaar to get subsidies or basic services. This pressure leaves many with no real choice and shuts some out altogether.

By connecting biometrics with financial and communication data, the system can track how people spend, where they move, and who they talk to—down to the smallest detail. Even when formal rules relax, the setup still leans toward holding everyone's data in one place, attached to their identity, not as anonymous records. This goes against what the Puttaswamy judgment wanted: less data collected, more control for individuals, and real privacy.

COMPARATIVE TECHNOLOGICAL PERSPECTIVES

A. Apple Pay and Tokenisation

Apple Pay really shows what privacy-by-design looks like in action. The system never stores your actual card number—neither on your phone nor on Apple's servers. Instead, it uses a unique token for your device and creates a new cryptogram for every transaction. Merchants and service providers don't get enough information to piece together your full transaction history. Even Apple can't see exactly what you bought.

This setup limits both corporate tracking and government surveillance, but it doesn't sacrifice security. Privacy isn't just a promise here—it's baked into the technology itself. Apple Pay

proves you can build a secure, functional payment system without giving anyone a constant window into what users are doing.

B. UPI and Traceability

India's Unified Payments Interface (UPI) puts traceability front and center. Sure, users see virtual payment addresses instead of account numbers, but every transaction ends up recorded in banking systems and NPCI databases. Law enforcement doesn't struggle to connect UPI IDs to real identities—they just follow set procedures and get the information they need.

Regulators care most about encryption, stopping fraud, and making sure everyone follows AML and KYC rules. Anonymity? Not really a priority. That means even small payments between friends leave a permanent, trackable record. Looking at this from a constitutional angle, you hit a big question: is it really necessary to track every transaction, no matter how minor, just to fight crime or collect taxes? The answer isn't obvious, and the balance feels off.

EMERGING PRIVACY THREATS

Mobile apps promising more security or convenience have exploded, but they come with bigger privacy risks. Both government and private apps ask for all sorts of permissions. They bury the details in long privacy policies, counting on people to get tired and just click "accept." Take Sanchar Saathi—this app shows how opt-out setups and government carve-outs end up dumping responsibility on the user.

Look at Truecaller. The company builds its database straight from users' contact lists, grabbing information about people who never even signed up. No real enforcement means this sort of thing becomes normal—companies just scoop up and sell personal data, and people lose control over their own information.

The line between corporate tracking and government surveillance keeps getting blurrier. Governments now lean on private databases and analytics, mixing public and private power. And with no independent regulator with teeth, both sides keep taking advantage of the imbalance. They hold most of the power and information. Ordinary people are left exposed.

LEGAL GAPS AND STRUCTURAL CHALLENGES

Three big problems stand out. There's no truly independent data protection authority, so people don't trust enforcement. The ways to get redress are scattered and hard to use, especially if the harm comes from state systems. On top of that, the state carves out huge exemptions for itself and skips mandatory privacy impact assessments, making surveillance routine and barely questioned.

Courts haven't stepped in with clear, technology-specific rules for things like UPI or government surveillance apps. As a result, the principles from Puttaswamy just sit there—they aren't shaping how these systems work in practice.

RECOMMENDATIONS

Reforms start with making sure the Data Protection Board runs independently, both in function and in daily operations. Payment systems need privacy-by-design built in from the ground up—things like tokenisation and smarter rules for how long they keep data. Government surveillance apps can't just go unchecked. They need to face strict privacy impact assessments, real public input, and outside audits. Courts should take a hands-on approach, enforcing proportionality and demanding clear, evidence-backed reasons for any intrusive digital setups.

CONCLUSION

After Puttaswamy, privacy isn't just a policy—it's a constitutional promise. Still, India's digital systems keep leaning toward surveillance and control, not individual dignity or autonomy. Other countries have shown that technology can protect privacy when it's built into the design. If India takes Puttaswamy seriously, it needs to do more than just acknowledge privacy on paper. Privacy has to shape the code, the institutions, and the routines of digital life.