The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

PRIVACY RIGHTS AND SOCIAL SURVEILLANCE IN CONTEMPORARY INDIA.

-Yashika Panwar

ABSTRACT

India's digital boom hasn't just made life more connected. It's also brought a flood of new tech that tracks people by the state, by businesses, pretty much everywhere. Take the biometric systems: they decide who gets food or welfare. Or the facial recognition cameras popping up in public places. Or laws that hand huge interception powers to government officials, with little real oversight. Surveillance in India keeps growing, and honestly, the rules meant to protect everyone can't keep up. This paper digs into the clash between the constitutional right to privacy which the Supreme Court cemented in the landmark Puttaswamy case and this rising tide of social surveillance. It pulls together legal debate, theory, and real-life stories to show something blunt: surveillance isn't some neutral force. It hits women, Dalits, minorities, and rural folks the hardest. And sure, the Digital Personal Data Protection Act of 2023 sounded like progress, but it still leaves big loopholes in those same old exemptions that stop anyone from actually holding surveillance accountable. In the end, the paper doesn't just throw up its hands. It offers solid steps for fixing the mess.

INTRODUCTION

It’s strange, almost quietly shocking, that in India, if you need subsidized grain from the Public Distribution System, you have to press your finger or look into a government scanner before you’re allowed to eat. Officially, the Aadhaar-linked food program says this biometric system stops fraud. But for a seventy-three-year-old woman in rural Jharkhand, whose work-worn fingers never seem to match the machine, or for a daily wage laborer turned away because they can’t get “authenticated” that day, the process feels very different. For them, survival now depends on passing a surveillance checkpoint.

This isn’t just one unusual story. It’s part of a bigger trend. Over the last ten years, India has put together one of the world’s largest surveillance networks. There’s biometric identity, tied into welfare programs, banking, and taxes. Cameras with facial recognition scan travelers in airports, track people at railway stations, even monitor more and more public spaces. Surveillance laws give the government broad powers to monitor calls and emails, with barely any judge involved. And now the plans are getting even bigger: proposals for a centralized data grid under NATGRID, plus the Crime and Criminal Tracking Network & Systems (CCTNS). Authorities claim all these measures are for security or to stop corruption. But they also open a flood of worries about privacy, about basic fairness, and about how surveillance bears down hardest on people already pushed to the margins. In 2017, the Supreme Court’s nine-judge bench settled the privacy debate. In Puttaswamy, they declared privacy a fundamental right under Article 21 of the Constitution. It was a huge moment, probably the most significant constitutional decision of the decade. But a big ruling doesn’t automatically change things. Four years later, India still had no solid data protection law. When the Digital Personal Data Protection Act finally landed in 2023, it included sprawling state exemptions. Critics weren’t convinced; they called it a surveillance law pretending to speak the language of privacy.

This paper takes a close look at India’s position on the issue. First, it digs into the legal setup of surveillance exploring the statutes, cases, and regulatory frameworks that spell out what the state and private players can actually do with personal data. Then, it turns to the social side: Who pays the most for surveillance, and how do inequalities caste, gender, class shape the experience of being watched? The paper wraps up with a set of reform suggestions, not arguing for the total abolition of surveillance. It's not realistic and, in some cases, not even desirable but pushing to make it more accountable, proportionate, and faithfully aligned with the constitutional principles set out in Puttaswamy.

LITERATURE REVIEW : FROM PRE-PUTTASWAMY AMBIGUITY TO THE DPDP ACTS GAPS

Privacy law in India hasn't followed a straight path. Right after independence, nobody really knew where privacy stood in the Constitution. In 1954, the Supreme Court took up M.P. Sharma v. Satish Chandra. The bench eight judges decided that there's no right to privacy in the Indian Constitution the way the U.S. has under its Fourth Amendment. Fast forward ten years, and the Court took another look in Kharak Singh v. State of U.P. The majority said the government couldn't just barge into someone's home for surveillance. But they hesitated to call that protection a standalone right to privacy. So, for a long time, privacy law in India was murky: some government actions were off-limits, but judges hadn't really nailed down why.

Over the next few decades, courts started recognizing privacy here and there in cases about bodily autonomy, sexual freedom, or the sanctity of the home. But they never quite answered the big, foundational question. As all this legal uncertainty dragged on, technology was changing everything. In the 1990s and early 2000s, privacy was more urgent than ever due to the digital communications boom. India passed the Information Technology Act, 2000, which actually gave the government legal tools to intercept digital conversations. Then, in 2008, they strengthened these powers even further. Privacy concerns just kept piling up, and the law struggled to keep pace. Academic writing on this era keeps circling back to a familiar problem: lawmakers kept using old rules, shaped for past surveillance tools, to govern new technologies. Oversight barely existed, and when it did, it sat firmly in the hands of the executive. There was almost no independent scrutiny. Usha Ramanathan's research on Aadhaar really brings this out. She shows how Aadhaar started as a voluntary program with a limited scope, but officials expanded it again and again. Each time, they used bureaucratic orders, not open legislative discussions. Gradually, it became mandatory for all sorts of government services. The big selling point, at least in public debate, was efficiency and welfare benefits. Almost nobody paid attention to the surveillance angle: connecting biometrics to services meant the state could keep close tabs on people's movements and activities, not just now but over time.

Feminist research gives us another perspective. Analysts looking at gender and surveillance in India highlight that digital tracking often reinforces old patriarchal controls and sometimes

makes them even more intense. For example, when women access services through Aadhaar, their movements, transactions, and even identities become more visible not just to the state, but through leaks and informal access, to family members or community leaders. That's a sharp contrast to the official narrative, which treats surveillance as empowerment ("your own" bank account, "your own" identity). In reality, these systems can turn into new tools for monitoring and controlling women.

Caste-focused studies add yet another dimension. Technologies like facial recognition, built mainly on upper-caste, urban, male faces, struggle when scanning darker skin, Dalit features, or women's faces. What happens? The system spits out more errors, more false positives, more innocent people wrongly flagged and detained. And it's exactly the communities that already suffer most from state discrimination that end up facing the brunt. This isn't just a technical flaw; it's a symptom of deeper social bias coded right into the technology.

Puttaswamy changed everything for privacy law in India. All nine Supreme Court judges agreed that privacy is a fundamental right, but they each got there in their own way. Justice D.Y. Chandrachud's concurring opinion really caught people's attention, especially when it came to government surveillance. He saw informational privacy, the right to decide what happens to your own data, as a core part of fundamental rights. He made it clear: government surveillance can't just run wild. It has to follow four strict rules: legality, a real purpose, proportionality, and proper safeguards. That proportionality test in particular now shapes how courts look at surveillance cases.Fast forward to the Digital Personal Data Protection Act, 2023. This law arrived in the world Puttaswamy built. It promised to give people more control: strong consent rules, clear rights for anyone whose data is being used, and a new Data Protection Board. But here's the hitch Section 17 hands the government a pretty big escape hatch. If the government says it's acting for sovereignty, security, foreign relations, or public order, it can exempt any agency from the law's protections. The language is vague, almost clipping straight from the broad terms of Article 19(2), which the state has always leaned on to defend all kinds of restrictions. Critics aren't buying it. They worry that if the government can pull the "national security" card whenever it wants, the whole law falls apart. At the end of the day, the government can keep itself out of the law's reach leaving people's privacy hanging by a thread.

THE LEGAL FRAMEWORK OF SURVIELLANCE : STATUES, CASES, AND GAPS

A. The Statutory Architecture

India's surveillance laws aren't exactly one coherent framework, but a patchwork of colonial and recent acts, which somehow manages to still function, just barely, more than a hundred years on. The foundational law is the Indian Telegraph Act, 1885, still the primary legislation concerning wiretaps and interceptions. Section 5(2) of the Act permits interception orders if the competent authority deems it "necessary or expedient in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order." These are vague terms, and scrutiny beyond a low bar isn't afforded. Interception orders are issued by the Home Secretary (central or state) and vetted by some bureaucracy, no courts required. More recently, in 2000, the IT Act stepped in. Section 69 mirrors the powers available under the Telegraph Act but extends them to communications through the internet-emails, chats, etc. Any government agency is now empowered to intercept or decrypt digital information if its deemed necessary or expedient in the interest of India's sovereignty, security, defense, friendly relations with foreign states, or public order. Again, authorization comes from higher up the executive hierarchy and never from a judge. Though the IT rules published in 2009 stipulated certain procedures, there is general consensus that safeguards were weak; for example, there was no obligation to ever inform a citizen that they were being monitored, not even in retrospect.
Fast forward to 2016 and the Aadhaar Act; India's first comprehensive biometric ID system was set up. While legislators attempted to protect citizen privacy with certain stipulations like only using Aadhaar data for the purpose it was meant for and making it a list of protected data types; the law also made provisions for a "request data" database and, with successive amendments and executive orders, Aadhaar data usage sprawled beyond legislative intent-often without coming before Parliament.
Finally, in 2023, came the Digital Personal Data Protection Act. While commentators are already raising concerns about loopholes and the state's exclusion, it must be seen as a victory of sorts for private players in terms of new privacy provisions such as consent, the right to erasure, and data minimization. All of this comes at a time when there was no substantive data law in India; however, this Act seems to disproportionately burden private parties with data protection, whereas the state has the power to accumulate vast amounts of personal data, and can give itself free rein whenever necessary.

B. The Constitutional Framework After Puttaswamy

The Puttaswamy judgment did not quash a particular surveillance program, but was restricted to the issue of whether the right to privacy is a fundamental right. But the proportionality test enunciated in the judgment has since been repeatedly referenced in judgments and academia as the touchstone for testing surveillance. Justice Chandrachud enunciates that to satisfy the proportionality test, an invasion of privacy has to be: lawful; pursue a legitimate state aim; proportional (least restrictive means possible to achieve the aim); and procedurally fair. However, when applied to the current Indian surveillance architecture, this leads to an overwhelming condemnation. The interception provisions of the Telegraph Act have been argued as "sanctioned by law" although not requiring a judicial warrant or any notification requirement. Similarly, IT Act provisions suffer from a similar lack of judicial oversight. The compulsory linking of welfare services to Aadhaar, that was later upheld by the majority of the SC in Puttaswamy II (2018) was criticised as applying an unconvincing lenient proportionality test that had yielded to efficiency arguments by the state.

The table below summarizes the key legislative and judicial instruments, their provisions relevant to surveillance, and the privacy tensions each creates:

Law / Case - Key Provision & Privacy Tension

Indian Telegraph Act, 1885 - 5(2): Executive interception orders : No judicial authorization; no notification requirement

IT Act, 2000, 69 - Executive orders for interception / monitoring : Broad exemptions; no sunset clauses.

Aadhaar Act, 2016 - Biometric enrollment linked to welfare : Mandatory linkage; data leakage risks |

Puttaswamy I (2017) - Privacy as fundamental right; proportionality test : Landmark but not self-executing |

DPDP Act, 2023 - Data protection framework; consent requirements : State exemptions; no judicial data access oversight

C. Facial Recognition Technology and the Surveillance Frontier

One striking manifestation of the mismatch between the theory of constitutional law and the practice of surveillance is facial recognition technology. While the Indian and many state governments have implemented the use of FRT in airports, train stations and public places, they have also planned significant expansions. The Telangana government, for instance, implemented the use of FRT for policing activities; the Delhi Police have employed face recognition to identify protestors. No laws in India regulate the use of facial recognition technology; prior privacy impact assessments are not required; independent oversight is lacking.

These features have enormous sociological consequences. Face recognition for policing is inherently biased: because its error rate is significantly higher when dealing with darker skin tones and women's faces, the consequences of misidentification-being mistaken for a suspect, subjected to heightened surveillance, or unjustly apprehended-will be disproportionately borne by groups already vulnerable to police harassment. The concerns regarding this disparate impact are not hypothetical: empirical evidence of this effect from similar systems used in the US and UK have been documented, and these programs are increasingly facing calls to regulate this effect. Indian agencies are deploying such systems while foregoing even the procedural and oversight mechanisms that have been implemented in those jurisdictions to address these problems.

IV. SOCIAL SURVEILLANCE THROUGH A SOCIOLOGICAL LENS: CASTE, GENDER, AND THE WATCHED BODY

A. Foucault, Surveillance, and India

While Michel Foucault's idea of surveillance as a technology of power-the panopticon as a metaphor not for prisons alone but for the entire disciplinary society-provides an interesting theoretical entry point, it must be adjusted slightly for the Indian context. Foucault's model assumes a seemingly undifferentiated subject; the prisoner who does not know if they are watched at any particular point and hence Internalizes the gaze continuously. In India, the experience of surveillance is highly differentiated according to caste, gender, class, and religion; the state is not equally watching us all. Some of us are being watched intensely and suspiciously and others, barely at all. This is not an error, not a malfunction, but a feature. Surveillance systems are human creations, fed by existing data structures, and deployed through

institutions-the police, the bureaucracy, the welfare machine-that have carried their own biases with them into the new systems. The effect of this in India is that surveillance tends to exacerbate, rather than disturb, hierarchies of power.

B. Gendered Surveillance

Welfare, Data, and Control Surveillance and gender are intertwined in India on multiple registers. At the level of the state, digital welfare programs were put in place as a form of women's empowerment; the Jan Dhan Yojana, for example, created hundreds of millions of new accounts, many of them for previously financially illiterate women who were given an "independent identity" with the subsequent Aadhaar linkage. However, the data generated by these accounts-transaction histories, location data, welfare claims-is readily available to family members, village officials and others in ways that replicate patterns of control. Researchers have found instances where the Aadhaar-linked accounts were controlled by male relatives and women's welfare entitlements redirected. The surveillance component (the fact that the woman's movement and transactions had suddenly become legible through the digital system) often did not empower the woman but made her more visible and available for others' control. At another level, the surveillance of women's online activities through social media monitoring, use of IT Act provisions to prosecute women for "offensive" content, or misuse of private images as a threat are dimensions of gendered surveillance. Though the law (the relevant section of the IT Act) appears gender-neutral, it is often women who bear the brunt of the actual prosecution; they are the primary victims in cases of cyber stalking, and their recourse-the existing legal channels, which require intense personal data disclosure, are often ineffective-makes them objects of a secondary level of surveillance.

C. Caste, Policing, and the Surveillance of Marginalized Communities

In India, the convergence of caste and surveillance perhaps finds its most obvious manifestations within the practice of policing. The colonial-era Criminal Tribes Act, 1871 – by which communities were declared 'criminal by birth' has long been repealed in name (it was withdrawn in 1952), yet its spirit continues in the Habitual Offenders Acts retained in nearly every state. By labeling specific communities which happen to be predominantly Dalits, Adivasis, and nomadic groups – as inherently criminal, these laws grant heightened surveillance rights and registration

burdens to their members. The surveillance apparatus of the 21st century, therefore, in some sense, upgrades that colonial structure. When applied to the practice of policing, the use of FRT becomes particularly problematic in terms of caste dynamics. Dalit activists and journalists have already documented numerous instances in which facial recognition systems have wrongly flagged Dalit individuals as suspects in criminal cases, with resulting arrests and police intimidation. This technology, in essence, encodes and scales bias: in its training data, its deployment patterns, its lack of meaningful recourse.Similarly, Aadhaar exclusions have been disproportionately experienced by marginal groups. The requirement for biometric verification - either by fingerprint or iris scan- posed a challenge to agricultural and construction laborers whose fingerprints were too worn to be captured, or for Dalits. In this case as in so many others, a 'technical' failure represents social failure, enacting exclusion along lines of social hierarchy.

D. The Muslim Community and Religious Surveillance

There are documented instances of surveillance of India's Muslim minority-of phone calls being intercepted, of religious congregations being monitored, of CCTNS data being used to mark whole communities as potential security risks-reported by civil society groups and journalists. In fact, the NRC exercise in Assam which risked rendering hundreds of thousands of residents who had lived there for decades stateless-as they could not prove their citizenship through documents-was a form of administrative surveillance resulting in untold human pain. The potential rollout of NRC-like exercises elsewhere-and the accompanying political discourse-created an environment where surveillance itself poses an existential threat for a part of the population that a more privileged section cannot even perceive. The CAA-NRC protests in 2019-2020, and their subsequent development is particularly illuminating in this regard. The deployment of facial recognition technology by Delhi police for identifying protest attendees-in the course of protests, which were largely peaceful, and largely populated by Muslim students and citizens-highlighted how surveillance mechanisms created, and legitimized, under the garb of one reason-public security-can be utilized for the purpose of political surveillance of dissenting voices.

V. THE PEGASUS AFFAIR AND THE LIMITS OF LEGAL ACCOUNTABILITY

No study of surveillance in India in the early twenty-first century can pass over the Pegasus scandal. In July 2021, international journalists reported a finding of the Pegasus Project, stating that the mobile phones of Indian journalists, activists, political opponents and government officials "appeared on a list of potential targets for the Pegasus spyware developed by the Israeli firm NSO Group." Pegasus is a 'zero-click' spyware, which means "it is capable of infecting a device with no action by the target and gives the user access to all messages, calls, e-mails, photographs and microphone on a targeted device."

The Indian government failed to affirm or deny the procurement and usage of Pegasus. After a public interest litigation (PIL), the Supreme Court appointed a technical committee that was tasked with examining the complainant's phones and finding out if Pegasus was used to attack them. Although the report of the technical committee was inconclusive-it could not "establish who was behind the attack with certainty"-and submitted in 2022, the Court noted that "lack of cooperation from the Government on the investigation was disturbing."

The Pegasus scandal captured some specific aspects of India's surveillance accountability crisis. First, there is no form of external scrutiny on the government's usage of surveillance technologies. The executive monitors its own interception orders. Parliament does not have any permanent committee to look after surveillance issues. Although the judiciary has at least shown willingness to scrutinize surveillance-in Pegasus, for example, by constituting a technical committee-it is in an ill-suited position to perform ongoing oversight of intelligence activities.

Second, there is no legal framework for spyware as a category. The Telegraph Act and IT Act only account for surveillance conducted by the state, or on its behalf by service providers. Direct malware on a target device is a different issue, as it circumvents service providers entirely. The DPDP Act does not help because it concerns data protection by fiduciaries.

Most significantly, the affair highlighted the extreme difficulty for individuals to gain redressal for targeted surveillance. Despite the Supreme Court intervention and global media coverage, no charges were brought, no program was acknowledged, no reform was enacted. For potential future targets of surveillance, the lesson of the Pegasus episode is: the government can spy on you, you will never know about it, and nothing will happen when it does.

VI. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: PROMISE AND BETRAYAL

Finally, after years of drafting and consultation, the DPDP Act finally materialized in early 2023 with an ambivalent welcome from the privacy community. Having operated for years without any meaningful data protection statute, the Act has established a normative framework: consent requirements for data processing; rights for data principals (like the right to access, and the right to erasure); obligations for data fiduciaries (like data security requirements and data breach notifications); and a Data Protection Board with adjudication and penalty powers. The consent mechanism will work as intended for private sector data processing; when a company wants to process personal data for targeted advertisements, in principle, it requires consent that is specific, informed, and revocable. And a data principal will have the right to erase data once consent is revoked. These are meaningful rights, though the efficacy of these rights will depend greatly on the powers and responsiveness of the Data Protection Board and the readiness of the individuals to invoke them. But the provisions that allow the State to bypass these requirements is a different story. Section 17(2)(a) of the DPDP Act, provides that the Central Government may exempt any government entity from any provision of the Act, without the need for proportionality review, judicial authorization or parliamentary oversight. And the grounds on which this exemption may be granted are vast: sovereignty, national security, public order, prevention of commission of any cognizable offence.

The grounds are so broad that almost any type of government data processing can be exempted. This has major practical consequences. India's social welfare system, including its vast Aadhaar, Jan Dhan, Direct Benefit Transfer architecture, manages sensitive data of millions of Indians. Similar concerns can be raised about the health data of beneficiaries of Ayushman Bharat Digital Health Mission, transaction data generated by UPI, location data, etc. So, all these could potentially be processed by government entities without meeting any data protection requirements. This asymmetry is problematic; it is philosophically incoherent and harmful. It ensures that the most powerful data processors of all-the state-face minimal regulation and the communities most at risk-the poor and marginalized, those who rely on state benefits- are the most unprotected. If the promise of Puttaswamy is to be fulfilled, section 17 of the DPDP Act must be amended radically.

VII. REFORM PROPOSALS

From the foregoing discussion, a number of reforms seem to be both necessary and feasible.

Independent Surveillance Oversight. India requires a statutory independent oversight mechanism for surveillance-analogous in function, adapted for India's constitutional context, to the Investigatory Powers Commissioner's Office in the UK, or the independent review mechanisms designed in Germany and Canada. Such a body needs to be constitutionally independent of the executive; composed of individuals with technical and legal competence; authorized to conduct ex post judicial reviews of interception warrants; and mandated to publish annual reports on transparency. Legislative oversight must be bolstered through parliamentary committees active in oversight of intelligence activities.

Judicial Authorization for Surveillance. An executive authorization system, where a state-sanctioned Home Secretary orders surveillance of Indian citizens, is irreconcilable with the proportionality standards in Puttaswamy. India must move toward a judicial warrant system requiring the prior authorization of an independent judge before surveillance, particularly content interception, occurs. This will bring India in line with most constitutional democracies and give substantive effect to the proportionality analysis outlined in Puttaswamy.

Regulation of Facial Recognition Technology (FRT). Until dedicated FRT legislation is introduced, courts and the Data Protection Board can employ existing constitutional and data protection laws to require necessity, proportionality, and impact assessments for all deployments of FRT. Parliament must eventually adopt FRT-specific legislation that demands: public and segregated accuracy testing results on the basis of skin tone, gender, and age; the banning of FRT deployment where the margin of error poses unreasonable risks; and accountability for wrongful identification. Modification of DPDP Act, S.17. An amendment to the state exemptions provisions of the DPDP Act should mandate that any government exemption be: based on a clearly articulated statutory necessity; proportionate to its objective; subject to a specific time limit; reviewable by a court of law; and requires the informing of Parliament. Exemptions should not serve as broad shields for all government surveillance schemes.Remedies for Surveillance-Affected Communities. The state should develop and fund targeted legal aid and awareness programs for communities most affected by surveillance: Dalits, women, religious minorities, and persons disenfranchised by biometrics failure in the context of state welfare systems. The right to information on surveillance should be actionable, establishing clear and

straightforward mechanisms for individuals to ascertain whether or not they have been subjected to state surveillance.

VIII. CONCLUSION

In the abstract, privacy is a value that almost anyone finds easy to embrace. What is difficult is implementing it-being willing to accept the costs (both administrative and in terms of security trade-offs) of effective privacy protection. India's surveillance architecture is a statement of choices-choices that have elevated executive efficiency over judicial control; that have constructed welfare systems that collect vast amounts of data without proper safeguards; that have introduced a potent array of biometric and facial recognition technologies without corresponding accountability measures for their power. These choices have not fallen equally upon every citizen. They have fallen hardest upon the least powerful among us: women navigating welfare systems that made them susceptible to exploitation rather than security; Dalit laborers for whom worn-out fingerprints could mean exclusion from sustenance; Muslim citizens for whom the specter of a surveillance state was far from hypothetical, but immediate and terrifying. The humanization of privacy law necessitates engaging with these lived experiences-not as ancillary policy points, but as core evidence for the material impact of surveillance.

Puttaswamy provided a foundation for constitutional privacy rights in India that is unquestionably world-class. A nine-judge bench unanimously affirmed privacy as a fundamental right. The proportionality test that they developed is substantively exacting. Building institutions, rules, and accountability structures that translate this into practice will be key to load-bearing that foundation. Current versions of both the DPDP Act and the Telegraph Act fail to do so. A complete lack of judicial authorization for surveillance, an absence of meaningful independent oversight, and the breadth of the state exemptions, all culminate in the normalization of surveillance with accountability becoming the exception.

It is not solely a matter that the law can fix. Surveillance has deep roots in our political economy, in the self-interest of governments to use surveillance technologies, in the commercial advantage that tech companies derive from them, and in the reproduced social hierarchies of caste and patriarchy that surveillance reinforces. Legal change is essential, but not sufficient; we also need

a public culture that considers privacy a democratic value and is willing to demand accountability from the government on its surveillance practices, protect journalists and activists exposing abuses, and reject the seductive but fallacious trade-offs of privacy for security or convenience. A surveillance state is not preordained. But to avert one, we must acknowledge its actual cost and to whom it falls.

REFERENCES

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Jean Drèze & Reetika Khera, *Dissenting on Aadhaar: Big Data Meets Big Brother*, Economic and Political Weekly (2017), documenting exclusion errors in Aadhaar-linked welfare systems.

Puttaswamy, (2017) 10 SCC 1, 248-650 (per Chandrachud, J.).

Usha Ramanathan, *The DPDP Act and the Surveillance State*, The Hindu (Sept. 15, 2023), noting that the state exemptions in the Act replicate the surveillance-enabling gaps of prior legislation.

M.P. Sharma v. Satish Chandra, (1954) SCR 1077.

Kharak Singh v. State of U.P., (1963) 1 SCR 332.

Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148; R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

Information Technology Act, No. 21 of 2000, § 69 (India).

Usha Ramanathan, *A Unique Identity Bill*, Economic and Political Weekly, Vol. 45, No. 30, at 10 (2010).

Amba Salelkar, *Aadhaar and Gender: How Biometric Authentication Misses Women*, 53 Economic and Political Weekly 1 (2018).

Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Machine Learning Res. 77 (2018) (documenting differential error rates in facial recognition across skin tone and gender; analogous concerns apply to Indian deployments).

Puttaswamy, (2017) 10 SCC 1, 648 (Chandrachud, J., concurring).

Digital Personal Data Protection Act, No. 22 of 2023 (India).

Digital Personal Data Protection Act, No. 22 of 2023, §§ 6-28 (India)

See Vrinda Bhandari & Faiza Rahman, *An Analysis of India's Digital Personal Data Protection Act, 2023*, Centre for Internet and Society (2023).

Indian Telegraph Act, No. 13 of 1885, § 5(2) (India).

Information Technology Act, No. 21 of 2000, § 69 (India).

Centre for Internet and Society, *Surveillance Law in India*, in The Surveillance Law Landscape in India (Gus Hosein ed., 2023), at 12-15.

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016 (India).

Digital Personal Data Protection Act, No. 22 of 2023, §§ 6-13 (India) (setting out consent requirements and data principal rights).

Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* 189-212 (HarperCollins India 2019).

Puttaswamy, (2017) 10 SCC 1, 648 (Chandrachud, J., concurring) (articulating a four-part proportionality test requiring legality, legitimate aim, necessity, and procedural safeguards).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (upholding the Aadhaar Act with modifications).

Internet Freedom Foundation, *Facial Recognition Technology in India: A Practical Assessment* (2022), documenting over 150 FRT deployments by central and state governments.

Alok Prasanna Kumar, *The DPDP Act and the Surveillance State: Five Key Concerns*, Vidhi Centre for Legal Policy (2023).

Buolamwini & Gebru, *supra* note 11, at 80-83.

Michel Foucault, *Discipline and Punish: The Birth of the Prison* 195-228 (Vintage Books, 2d ed. 1995).

Ministry of Finance, Government of India, *Pradhan Mantri Jan Dhan Yojana: Progress Report* (2023).

Reetika Khera, *Impact of Aadhaar on Welfare Programs*, 52 Economic and Political Weekly 61 (2017).

Debarati Halder & K. Jaishankar, *Cyber Victimisation of Women by Online Sex Offenders: Empirical Study*, 2 J. of Victimology & Victim Justice 1 (2019).

Meena Radhakrishna, *Dishonoured by History: 'Criminal Tribes' and British Colonial Policy* (Orient Longman 2001).

Internet Freedom Foundation, *supra* note 24, at 14-16.

Jean Drèze & Anmol Somanchi, *The COVID-19 Crisis and the Public Distribution System*, 56 Economic and Political Weekly 35 (2021) (documenting biometric authentication failures for agricultural laborers).

Amnesty International India, *Designed to Exclude: How India's Biometric ID System Fails Marginalised Communities* (2018).

Siddharth Varadarajan & Siddharth, *The Pegasus Project: How India's Government Uses Spyware*, The Wire (July 2021).

Forbidden Stories & Amnesty International, *Pegasus Project: Technical Methodology Report* (2021).

Manohar Lal Sharma v. Union of India, (2022) 7 SCC 535.

Digital Personal Data Protection Act, No. 22 of 2023, 6-28 (India).