The *Aadhaar* Verdict and the Surveillance Challenge

Ananth Padmanabhan & Vasudha Singh***

Abstract *Conventional responses to privacy protection, such as the notice-and-consent framework, are inapposite to a datafied world where ubiquitous data collection is facilitated by a range of advanced technologies. Such traditional frameworks also commonly vest the State with more leeway than private companies to access personal data, which amplifies privacy harms in case of State use of data. Despite the ominous possibility of State surveillance, the Indian judiciary has thus far grappled with the right to privacy through a narrow lens focused on individual privacy risks rather than structural moves towards a surveillance society. This article explores a different viewpoint by studying the structural effects of the Aadhaar project on privacy, which drastically differ from the individual harms that Indian privacy jurisprudence is equipped to address. It first introduces the Supreme Court's engagement with the right to privacy through prior verdicts. It then explores the surveillance concerns raised by the petitioners in the Aadhaar verdict. This part examines the Supreme Court's response to these surveillance challenges and its failure to address structural inroads on privacy through architectural design choices that deliberately prescribe low baseline protection. Finally, the article contrasts this approach with the more holistic perspective on citizen-State interaction evident in Justice Chandrachud's minority view.*

* Dean, Daksha Fellowship.
** Advocate, Delhi High Court.

I. Introduction

Informational privacy[1] has become a fiercely contested dimension of privacy in recent times due to the trade-offs between ceding such privacy on the one hand and obtaining several benefits on the other. How societies handle data, be it in the realm of market behaviour or State functionalities, lies at the heart of this debate. Data can reshape market needs through personalised products and services, turn elections, and empower the State to track its citizens.[2] Standard responses such as the notice-and-consent framework do not appear robust enough to protect personal information in a datafied world.[3] This is often the case because the meaning and implications of elaborately worded privacy policies are lost on even legal experts. Additionally, this framework is ill-suited to the ubiquitous data gathering facilitated by more recent advances such as internet-of-things, radio frequency identification sensors, and commercial drones.[4]

These harms are amplified when it comes to the use of citizen data by the State. To begin with, the State is given more leeway than private companies when accessing data. A recent example of this differential treatment is seen in the case of Personal Data Protection Bill, 2019, which provides sweeping exemptions to the State for non-consensual data processing.[5] Most rely on larger public interest and State necessity as the foundational basis to do away with the consent requirement as well as, arguably, with other important privacy principles including data minimisation, purpose limitation, and

---

1 This branch of privacy, closely linked to the idea of 'informational self-determination', conceptualises individuals as rights-bearers with the authority to control their personal information and to determine how and when such information is communicated to others. *See*, Alan F Westin, *Privacy and Freedom* (1st edn, Athenum, 1967) 7. For a critique of this sole focus on control over personal information, *see*, Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087, 1109-1115. Solove argues for a bottom-up approach to define the concept, one that looks at specific technology-enabled intrusions and other encroachments into the personal information domain and the kind of harms that society desires to guard against. *See*, Solove (n 1) 1154-55.

2 Gautam Bhatia, 'Gautam Bhatia Dreams of Genuine Data Protection in India' (*LiveMint*, 11 August 2018) <https://www.livemint.com/Leisure/RuHOGczbrpt33v5ijP987M/Gautam-Bhatia-dreams-of-genuine-data-protection-in-India.html> accessed 19 June 2019.

3 Rishab Bailey and others, 'Disclosures in Privacy Policies: Does 'Notice and Consent' Work?' (2008) National Institute of Public Finance and Policy Research Paper No. 246 <https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf> accessed 19 June 2019; Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 I/S: A Journal of Law and Policy for the Information Society 543, 565.

4 Ananth Padmanabhan and Anirudh Rastogi, 'Big Data' in Devesh Kapur and Madhav Khosla (eds), *Regulation in India: Design, Capacity, Performance* (Oxford: Hart Publishing 2019).

5 Personal Data Protection Bill 2019, cls 35 and 91(2).

transparency.[6] Unfortunately, the risks arising from such dilution of meaningful safeguards are more pronounced when the might of the State is drawn into the equation.

David Lyon discusses the possibility of 'surveillance societies' that are orchestrated through a combination of technologies that monitor or intercept personal information. Lyon points out that we usually understand State surveillance as a monolithic, centralised panopticon. However, in reality, surveillance societies assemble several "*audio-visual protocols*" that converge "*discrete systems of surveillance*."[7] Moreover, in extreme cases, citizens and private actors are even enlisted by the State to collaborate in such mass surveillance.[8] The role of technology is central to the ominous possibilities that this new form of State power entails, as noted by Justice Sanjay Kishan Kaul in *K.S. Puttaswamy* v. *Union of India* (***'Puttaswamy'***).[9] Here, the learned judge rightly observed that "*surveillance is not new, but technology has permitted surveillance in ways that are unimaginable*."[10]

Protective legal frameworks have been a standard response to the interception of private communications by the State, though the nature of the response varies across jurisdictions.[11] Most such responses entail some form of judicial involvement in the interception of private communications by law enforcement authorities. For example, under Australian law, a warrant from a judge or a nominated member of the Administrative Appeals Tribunal is required to intercept private communications. But the procedure does not envisage any form of contestation over the grant of such warrant, perhaps

---

6 Madhav Khosla and Ananth Padmanabhan, 'Draft Data Protection Bill Pays Little Attention to the Dangers of State Power' (*ThePrint*, 30 July 2018) <https://theprint.in/opinion/draft-data-protection-bill-pays-little-attention-to-the-dangers-of-state-power/90511/> accessed 19 June 2019.

7 David Lyon, 'Surveillance, Power and Everyday Life' in P Kalantzis-Cope and K Gherab-Martín (eds), *Emerging Digital Spaces in Contemporary Society* (Palgrave Macmillan 2010) 107, 108-09.

8 Alexandra Ma, 'China is Building a Vast Civilian Surveillance Network – Here are 10 Ways it could be Feeding its Creepy 'Social Credit System'' (*Business Insider*, 29 April 2018) <https://www.businessinsider.in/China-is-building-a-vast-civilian-surveillance-network-here-are-10-ways-it-could-be-feeding-its-creepy-social-credit-system/articleshow/63959324.cms> accessed 19 June 2019. This is not a new phenomenon, as borne out by a historical examination of exercise of State power in several diverse situations in the past, and resort to legislative and executive action to pry into the lives of citizens. *See*, Westin (n 1).

9 *KS Puttaswamy v Union of India* (2017) 10 SCC 1 *(Puttaswamy)*.

10 ibid 618.

11 *See*, '2017 Surveillance Law Comparison Global' (*Baker Mckenzie*, 2017) <https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/2017_surveillance_law.pdf?la=en> accessed 19 June 2019.

with the intent of preserving the efficacy of this exercise of state power.[12] But these safeguards do not apply when monitoring metadata,[13] which is highly useful to combat crimes but equally powerful as a surveillance instrument. Contrast this framework with Germany, which permits surveillance by specific agencies like the Federal Intelligence Service without a prior judicial warrant sanctioning the same.[14] They must follow certain procedures while undertaking surveillance and intercepting communication but barring that, the collected information can be used to share intercepted intelligence for criminal prosecutions.

'Surveillance societies' defy even these standard safeguards because of mass surveillance programs facilitated through advanced snooping technologies. The Snowden leaks can be considered a watershed moment in our understanding of modern surveillance because it brought to public glare the enormous privacy intrusions that such programs could achieve through strikingly opaque means. Even when judicial orders are legally mandated before undertaking these exercises, courts have often granted such orders without any meaningful scrutiny, raising doubts over the efficacy of constitutional and legal safeguards against surveillance in the digital age. In India, surveillance is carried out through various methods, including telephone-tappingas authorised under the Indian Telegraph Act, 1885 and the amended Telegraph Rules, 1951. This legal framework allows interception of a "*class of messages*" sent to or from a "*class of persons*", thereby technically permitting mass surveillance so long as the other safeguards are satisfied.[15]

But most mass surveillance programs came about in the aftermath of the 26/11 Mumbai terror attacks that shook the nation. Prominent among these are the Central Monitoring System ('**CMS**') that acts as an automated centralised portal granting direct access to all communication data (including voice calls over mobile and landline, internet messaging, and metadata

---

[12] Surveillance Devices Act 2004, sub-ss 4 and 16.

[13] Broadly defined as "*data about data*", metadata includes basic information about any piece of data such as the name of the author, dates of creation and modification of files, file-size, search engine metatags, call records and tower location details. *See*, Bryce Clayton Newell and Joseph T Tennis, 'Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs' (iConference, Berlin, March 2014) <https://www.ideals.illinois.edu/bitstream/handle/2142/47299/109_ready.pdf> accessed 19 June 2019.

[14] *See*, the Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (G-10 Act).

[15] Indian Telegraph Rules 1951, R 419 A(4). Prior judicial approval has not been a feature in this framework, which relies on bureaucratic approval mostly from senior home ministry officials based on exigencies of the situation, when directing telecom service providers to intercept communications over their network.

on calls and internet usage) to security agencies of the State,[16] the National Intelligence Grid ('**NATGRID**'), the Crime and Criminal Tracking Network & Systems, and the Network Traffic Analysis System.[17] These programs have relied, for their legal basis, on amendments carried out in 2008 to the Information Technology Act, 2000, and IT rules that operationalised these newly conferred powers. But this framework mostly mimics the protective regime against unauthorised telephone-tapping,[18] which is realistically equipped, at best, to address individual privacy risks rather than regressive structural moves towards a surveillance society. As explained below, structural inroads on privacy involve a consciously low protection baseline through architectural design choices, and differ from case-by-case exemptions for State surveillance. The judicial engagement with surveillance in India, however, has mostly been within the latter context, one where the harms are again more immediately perceived than constituting themselves in the long run.

The recent verdict of the Supreme Court of India ('**Supreme Court**') in *K.S. Puttaswamy* v. *Union of India* ('***Aadhaar* verdict**') and its consideration of the plea that the Aadhaar project could enable mass surveillance by the State, must be appreciated with this background in mind.[19] The Aadhaar database, built up through practically non-consensual data gathering, envisages seeding Aadhaar numbers in multiple databases and thereby eases on-demand access to biometric and other sensitive information by State authorities. The project also entails authentication of subjects at various end-points to avail services and benefits, with records of such authentication events potentially offering a comprehensive account of a subject's interaction with the State and

[16] For a comprehensive discussion of this project, *see,* Addison Litton, 'The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression' (2015) 14 Washington University Global Studies Law Review 799.

[17] For an overview of these mass surveillance programs, *see*, Udbhav Tiwari, 'The Design and Technology behind India's Surveillance Programs' (*The Centre for Internet and Society*, 20 January 2017) <https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes> accessed 19 June 2019.

[18] *See*, Rishab Bailey et al, 'Use of Personal Data by Intelligence and Law Enforcement Agencies' (*The National Institute of Public Finance and Policy*, 1 August 2018) <http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf> accessed 19 June 2019. Bailey identifies three important aspects in which interception powers under the IT Act and Rules exceed similar powers in the Telegraph Act; Madhav Khosla and Ananth Padmanabhan, 'Both BJP and Congress are Complicit in Expanding State Surveillance without Legal Basis' (*ThePrint*, 24 December 2018) <https://theprint.in/opinion/both-bjp-and-congress-are-complicit-in-expanding-state-surveillance-without-legal-basis/168084/> accessed 19 June 2019.

[19] See, *KS Puttaswamy v Union of India* (2019) 1 SCC 1 (*Aadhaar verdict*).

even private entities.[20] These fears motivated the petitioners' constitutional challenge to the Aadhaar project as being, *inter alia*, violative of Article 21 because it presents the ominous possibility of a surveillance State.

Part II explores the nature of individual privacy risks that the Supreme Court has come to address through prior verdicts. Part III then proceeds to detail the specific surveillance concerns raised by the Aadhaar project and highlighted by the petitioners in this case. The Aadhaar challenge raised concerns that drastically differed from the individual harms that Indian privacy jurisprudence was equipped to address, as demonstrated here. This part then examines how the Supreme Court's majority opinion dealt with the surveillance challenge, and the gaps resulting from its lack of prior experience in dealing with mass surveillance. The final part contrasts this with the more holistic and structural perspective on citizen-State interaction evident in Justice Chandrachud's minority view. It concludes that a more robust review is required in cases of mass surveillance. Not only are the harms and consequences more long-term in nature, these cases usually involve technology design that pegs the privacy baseline at undesirably low levels.

II. Surveillance and the Supreme Court

The Supreme Court's understanding of privacy and surveillance has evolved through the years. But even in this progressive journey, judicial verdicts have primarily dealt with the right to privacy within the context of existing individual harms rather than architectural interventions and mass surveillance technologies that structurally altered the power balance between the repositories and recipients of State power. In *M.P. Sharma* v. *Satish Chandra*,[21] acts of search and seizure, carried out in pursuance of powers vested with investigative authorities under the Code of Criminal Procedure, were challenged on the basis that they violated the fundamental right to acquire, hold and dispose of property[22] and the fundamental right against self-incrimination.[23] When dealing with the right to privacy within this narrow setting, the court held that this right could not be imported to Indian jurisprudence

---

[20] For a comprehensive critique, *see*, Ananth Padmanabhan, 'The Three Sins of Aadhaar' (*Open Magazine*, 4 August 2017) <www.openthemagazine.com/article/essay/the-three-sins-of-aadhaar> accessed 19 June 2019.

[21] *MP Sharma v Satish Chandra* AIR 1954 SC 300.

[22] Constitution of India 1950, art 19(1)(*f*) — before it was deleted from the bouquet of fundamental rights vide the Constitution (44th Amendment) Act, 1978.

[23] Constitution of India 1950, art 20(3).

through a process of strained construction.[24] Though this was not a case of surveillance, its adjudicatory structure is no different from many others that followed, where the court determined the status or scope of the right to privacy under the Indian Constitution through a balancing of immediate individual harms against specific State goals rather than through an evaluation of systemic surveillance projects with long-term consequences.

This is evident from the very next case in this line of precedents dealing with the right to privacy. In *Kharak Singh* v. *State of U.P.*,[25] the Supreme Court dealt with the constitutionality of police surveillance that included 'domiciliary visits' from local police officials to the petitioner's house at night authorised *vide* Regulation 236(b), Chapter XX of the Uttar Pradesh Police Regulations. A six-judge bench of the Supreme Court invalidated this provision as violating Articles 19 and 21. However, the remaining provisions authorising 'surveillance' such as secret picketing of the residence of the "*history sheeter*" and maintaining a report of his habits, associations and movements, were upheld because "*the right of privacy is not a guaranteed right under our Constitution, and therefore the attempt to ascertain the movements of an individual is merely a manner in which privacy is invaded and is not an infringement of a fundamental right*." While the Supreme Court has now wholly discarded this view on the status of the right to privacy as borne out by the categorical and unanimous view to the contrary in *Puttaswamy*, the point we make here still holds. As Gautam Bhatia has pointed out, "*the State argued - and the Court endorsed - the basic idea that what makes surveillance reasonable … is the very fact that it is … targeted at individuals who are specifically suspected of being a threat to society because of a history of criminality*."[26] Thus, the adjudicatory structure was one calling into question the balance between immediate individual harms and state necessity.

Similarly, in *Malak Singh* v. *State of P&H*,[27] inclusion of the petitioners' names into a surveillance order was challenged because it was solely motivated by extraneous reasons rather than the prevention of crime as required under law. The petitioners relied on the right to privacy to contend that they ought to have been heard prior to their inclusion in this order. The Supreme Court disagreed, despite locating the right to privacy within the concept of individual dignity embedded in Article 21. It framed the dispute as involv-

---

[24] Gautam Bhatia, 'State Surveillance and the Right to Privacy in India : A Constitutional Biography' (2014) 26 National Law School of India Review 127, 128.

[25] *Kharak Singh v State of UP* AIR 1963 SC 1295.

[26] Bhatia (n 24) 129.

[27] *Malak Singh v State of P&H* (1981) 1 SCC 420 *(Malak Singh)*.

ing the extent to which the citizen's right to be let alone could be "*invaded by the duty of the Police to prevent crime*."[28] The court then proceeded to reason that a close watch over suspects was required to effectively combat organised crime.[29] Because effective surveillance had to be discrete, the court struck the balance in favour of the larger social goal of policing and disentitled the petitioners to a right of prior hearing.[30] The court also underscored provisions in the Police Rules that safeguarded individuals against unbridled exercise of surveillance power, and the option of judicial recourse against specific instances of such exercise.[31] Structural changes to the surveillance architecture were neither petitioned for nor *suo moto* considered in any of these cases.

The only case in this line of precedent that initially comes across as one where the Court addressed a structural problem is the verdict in *People's Union for Civil Liberties* v. *Union of India*[32] ('***PUCL***'). Here, a public interest litigation was initiated against the abuse of political power perpetrated through unchecked and illegal telephone tapping. The constitutional validity of Section 5(2) of the Indian Telegraph Act, 1885 was challenged. The Supreme Court declined to go into the constitutional validity of this provision, instead proceeding to discuss the executive's role in adhering to statutory pre-requisites such as the pre-conditions of 'occurrence of any public emergency' or situations that involved 'the interest of public safety' for the issuance of an interception order. Thus, on closer reading, this case similarly involved the balancing of unjustifiable immediate harms against justifiable state goals. The court's tackling of the matter through detailed directives did address some structural defects but was mostly a check on arbitrariness in the issuance of telephone tapping orders in specific cases. These directives demanded specificity of State action, be it the communications, persons or addresses intercepted, the exhausting of alternate and less intrusive ways to acquire the information before activating interception, and limiting intercepted material to the necessary minimum.

However, the existing technology at that point did not permit mass surveillance in the way that CMS and NATGRID now enable, thereby limiting judicial imagination of threats and consequences that went beyond immediate harms to the individual. Accordingly, these directives are inconsistent with mass surveillance and the kind of safeguards required to protect

---

[28] ibid 421.
[29] *Malak Singh* (n 27) 424.
[30] *Malak Singh* (n 27) 425-26.
[31] *Malak Singh* (n 27) 426.
[32] *People's Union for Civil Liberties v Union of India* (1997) 1 SCC 301.

innocent citizens in such cases.[33] Mass surveillance, especially the kind citizens are subject to in the present day and age, usually relies on technology design that keeps the baseline of privacy protection low, rather than on State action that makes use of exceptions to access data architecture or communication modes that are otherwise private. To illustrate, a directive that end-to-end encryption must not be deployed, or that the encryption key length must be kept low, is a vehicle for mass surveillance because it keeps privacy baseline low as a technological feature. The technology specifications become a part of any new product or service that is on offer because it is integrated as a design feature. Thus, such directives and measures have surveillance-by-design as their driving agenda, unlike telephonic communications where the inventor neither applied his mind to questions of surveillance or the best form of design that would enable such surveillance, nor was he compelled to do so by the State. By default, the design itself favoured and valued privacy and anonymity, with limited exceptions emerging with time.[34]

In similar fashion, requesting decryption assistance in individual instances – again a power that can be abused – would remain an exception to a system where the privacy baseline is still high. These examples are akin to telephone tapping because they do not address the core design principles in the technology itself, thereby conceding at a fundamental level that the design is in favour of privacy and anonymity and then devising exceptions to the workings of this design in suitable cases. In any case, they do not qualify as surveillance-by-design because the possibility of surveillance is not integrated as a design feature in the technology at hand. The *PUCL* directives were geared only to tackle the abuse of such exceptions, and not to evaluate technology design *vis-à-vis* the optimal privacy baseline for citizens and communities.[35] The court did not provide any guidance on assessing the design principles for any new technology that enables communications between individuals, for the straightforward reason that that was not the issue at hand.

Finally, in the most important verdict on the right to privacy in recent times, *Puttaswamy*, a nine-judge bench of the Supreme Court held privacy to be an expression of human dignity and therefore a vital part of fundamental rights guaranteed under the Indian constitution. This verdict is also important because of its focus on informational privacy, a dimension that

---

[33] *See*, Bhatia (n 24) 144.

[34] Edgar A Whitley et al, 'From Surveillance-by-Design to Privacy-by-Design: Evolving Identity Policy in the United Kingdom' in Kees Boersma et al (eds), *Histories of State Surveillance in Europe and Beyond* (Routledge 2014).

[35] For a comprehensive discussion on how many of the mass surveillance tools compromise the general level of privacy in electronic communications, *see*, Bailey (n 18) 16-17.

had not come to the forefront in a major way in earlier Supreme Court cases.[36] The court, for instance, recognised how people are increasingly spending more time on the internet and as a consequence, their digital footprints can "*reveal patterns, trends and associations, especially relating to human behaviour and interactions.*"[37] The court observed that this information can be used as a tool to exercise control over people and "*have a stultifying effect on the expression of dissent and difference of opinion, which no democracy can afford.*"[38]

But here too, the court's engagement with the right has been mostly focused on the balance between immediate individual harms and larger social goals. This is despite the broader context of structural surveillance under the Aadhaar program, which thus provided the Court ample opportunity to examine both the individual and structural aspects of privacy. Even its articulation of the limitations on privacy through proportionality assessments bears the strong imprint of this balancing exercise between individual rights and social goals. Justice Chandrachud's opinion articulated exceptions benefiting big data analytics for better governance, revenue utilisation, law enforcement and other social benefits.[39] However, it failed to probe deeper into the structural ramifications of such analytics in terms of the incentives they create, the manageability of such projects, and the essential line-drawing between responsible and unsafe innovation. For instance, Justice Kaul recognises that we are no longer contending with new forms of data alone, but also new methods to analyse and use such data with more effective algorithms and enhanced computational powers.[40] His opinion then registers reality as one where, in suitable cases, the collection and processing of big data would be legitimate and proportionate even when invasive of individual privacy, due to the ability of big data models to promote public interest.[41] At the same time, however, these models could very easily be made to work together to facilitate an undesirable 'surveillance society' in the future. The court failed to articulate any suitable legal safeguards to protect against these slightly more futuristic, yet quite real, harms. This in turn illustrates

---

[36] *See*, *R Rajagopal v State of TN* (1994) 6 SCC 632; *X v Hospital Z* (1998) 8 SCC 296; *Sharda v Dharmpal* (2003) 4 SCC 493. These cases, though dealing with privacy of personal information, were not constitutional cases in a real sense. The Supreme Court had erroneously constitutionalised these cases, which involved privacy intrusions by private individuals rather than the State. A possible exception is the verdict in *District Registrar & Collector v Canara Bank* (2005) 1 SCC 496, where the Stamp Act authorised the District Collector to access the confidential bank records of private individuals.

[37] *Puttaswamy* (n 9) 619.

[38] *Puttaswamy* (n 9) 620.

[39] *Puttaswamy* (n 9) 505.

[40] *Puttaswamy* (n 9) 619-20.

[41] *Puttaswamy* (n 9) 620.

how 'surveillance societies' often shape themselves in slow and discreet ways without raising immediate or obvious constitutional concerns.

In fact, a notable instance where the Supreme Court responded to some of these more long-term consequences was the verdict in *Shreya Singhal* v. *Union of India*,[42] a case dealing with free speech and not directly with the right to privacy. Here, the police had invoked section 66-A of the Information Technology Act, 2000 against some Facebook users for expressing their displeasure at a city-wide shutdown in Mumbai in the wake of Shiv Sena supremo Bal Thackeray's death. Striking down this provision as being unconstitutional for its chilling effects on the freedom of speech and expression, the court opened doors to the possibility of evaluating structural power imbalances brought on by vaguely worded criminal offences. Chilling effects can occur when the citizen apprehends that the State is watching her activities. While immediate criminal consequences may not necessarily follow, the mere existence of vague and overreaching criminal liabilities could restrain individuals from expressing themselves due to the fear of attracting such consequences. As the court reasoned,

> Section 66-A is cast so widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. Such is the reach of the section and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total.[43]

The court did not even consider reading down the provision, instead striking it down in its entirety.

While we do not argue here that the 'chilling effects' doctrine is a perfect mechanism to scope out the limits of state authority when undertaking mass surveillance, the verdict in *Shreya Singhal* demonstrated the need to evaluate possible long-term consequences of State action. To do so, the judiciary must necessarily go beyond immediate cases of rights infractions to a critical scrutiny of the architecture put in place, be it legal or technological. This is not a point exclusively limited to rights reviews. Even cases involving the dilution of judicial independence through the formation of tribunals, for instance, demand similar outlook. As do instances of colourable exercise of power such as law-making on a regular basis through ordinances. In all these situations, the State's usual defence that the scope for abuse is no ground to strike down an executive or legislative action, stands weakened. These are

---

[42] *Shreya Singhal v Union of India* (2015) 5 SCC 1 *(Shreya Singhal)*.
[43] *Shreya Singhal* (n 42) 167.

all architectural questions, ones that have a bearing on even the basic structure of the Constitution, but not in the same way that surveillance orders against history sheeters or individual instances of telephone tapping impinge on individual rights. But as the Aadhaar verdict reveals, courts are both less inclined and less equipped to make the evaluations that such architectural changes necessitate.

III. Aadhaar's Surveillance Risks and the Judicial Resolution

The petitioners in the *Aadhaar* challenge raised several concerns regarding the effect of this project on fundamental rights and the future of democracy. The collected information sufficiently indicated, in their view, the religion, class, social status, income, education, medical history, and other sensitive personal information relating to an individual and a further analysis of such data could even throw light on her habits, preferences and behaviour. Thus, it completely altered the balance of power between the State and its citizens.[44] The need for an Aadhaar database was justified by the State as primarily an exercise to ensure deliveries of subsidies and benefits to deserving beneficiaries through a de-duplication of fraudulent identities and a reliable process of identity verification.[45] The Aadhaar project worked through the gathering of vital pieces of information – biometric information including fingerprints, iris scans; demographic information including photograph, name, age, address, sex, mobile number, e-mail address, family members and their Aadhaar numbers; transaction metadata such as the frequency and purpose of authentication, the frequency of failure of authentication, and the device ID of the biometric capture device used for authentication; information to which the Aadhaar number was linked or seeded including bank accounts, income tax returns, scholarships, licences, voter card, etc.– though not all such information resided in a single database. The Unique Identification Authority of India ('**UIDAI**') submitted before the court that the project was built on the principles of minimal data, optimal ignorance, unidirectional linkage, and federated databases.[46] In simpler terms, the technology design was such that no central authority including the UIDAI had access to all the purposes for which the Aadhaar number was used. Thus, mere access to Aadhaar numbers did not provide knowledge on how citizens

---

[44] *Aadhaar verdict* (n 19) 437-38.
[45] *Aadhaar verdict* (n 19) 369-70.
[46] *Aadhaar verdict* (n 19) 227.

availed of other systems in which these numbers were seeded – tax, banking, pension, employment, to name a few.

Even assuming the UIDAI's contentions to be true, the challenge here was as much to the Aadhaar project as the Aadhaar Act and regulations thereunder.[47] Viewed from this lens, the wider project had spawned the creation of State Resident Data Hubs ('**SRDHs**') by various state governments, presenting the perfect tool to conduct mass surveillance. These data hubs, information pertaining to which was and still is mired in opacity, envisioned linking Aadhaar numbers with almost every state-sponsored scheme or payment from the state exchequer. They helped offer a 360-degree view of state residents, as publicly claimed by the State governments – Haryana, Andhra Pradesh, Tamil Nadu, Madhya Pradesh and others – that instituted such SRDHs.[48] While the SRDHs utilised Aadhaar information as their foundation, they failed to extend data protection and privacy safeguards envisaged under the Aadhaar act, to their operation.[49] Thus, even a basic enquiry into the procedures and systems in place with respect to the SRDHs made it evident that the aggregation of data from different silos, profiling, and consequential surveillance of residents was no longer in the realm of conjecture. Unique Aadhaar numbers made the findability of information much more convenient by serving as a unifying link for information held across various government departments and databases.[50]

To articulate this threat in legal terms, the petitioners relied on important decisions of the European Court of Justice ('**ECJ**') that appreciated state-sponsored surveillance systems as a separate class when coming up for judicial review. In most such cases, the applicant could not establish special harm or even conclusively demonstrate being subjected to any surveillance. Yet, in *Kennedy* v. *The United Kingdom*,[51] the ECJ held that the general

---

[47] *See*, the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act 2016.

[48] Anand Venkatanarayanan, 'The 360 Degree Database' (*Medium*, 5 December 2017) <https://medium.com/@venkatanarayanan.anand/the-360-degree-database-17a0f91e6a33> accessed 19 June 2019.

[49] All these databases are governed in the same manner as any welfare measure i.e. strictly through executive orders and resolutions, without appreciating the privacy risks that place them on a separate footing. *See*, Aman Sethi, 'Why State Data Hubs Pose a Risk to Aadhaar Security' (*Hindustan Times*, 13 March 2018) <https://www.hindustantimes.com/india-news/why-state-data-hubs-pose-a-risk-to-aadhaar-security/story-Klyl3yT5MkFk6Szg2yGg9N.html> accessed 19 June 2019.

[50] Annexure A, Submission of Ms Meenakshi Arora, Senior Advocate on behalf of the petitioners, *VickramCrishna v UIDAI* Transfer Case (Civil) No. 152 of 2013 decided on 26-9-2018 (SC) and *SG Vombatkere (SC) v Union of India* WP(C) No. 797 of 2016 decided on 26-9-2018.

[51] *Kennedy v United Kingdom* 2010 ECHR 682.

approach that denied individuals the right to challenge a law in the abstract based on its potential for abuse would not apply where secret surveillance took place. In such situations, courts had to apply a stricter standard, one that evaluated the availability of domestic remedies to effectively challenge acts of surveillance. The ECJ concluded so because in its view, "*the menace of surveillance can be claimed in itself to restrict free communication…, there by constituting … direct interference with the right guaranteed by Article 8*."[52]

Similarly, regarding substantive limits on surveillance programs, the ECJ provided adequate guidance, a point relied on by the petitioners in the *Aadhaar* challenge. Minimum legal safeguards were spelt out in *Roman Zakharov* v. *Russia*,[53] a case that challenged Russia's system of surveillance of mobile communications. These are:

> the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed.[54]

Evaluating Russian surveillance law against these benchmarks, the ECJ found that technical details pertaining to surveillance were not generally accessible to the public, despite impacting their right to privacy. The law suffered from overreach, permitting interception in respect of "*a very wide range of criminal offences, including … pickpocketing*", as well as "*of a person who may have information about an offence or … relevant to the criminal case*."[55] It also legitimised withholding necessary information from review proceedings meant to assess the legality of contested surveillance orders, thereby stripping such review of its efficacy.

Russian telecom service providers also had to mandatorily install equipment facilitating direct law-enforcement access to all mobile telephone

---

[52] *Roman Zakharov v Russia* 2015 ECHR 1065. In this case, the European Court of Justice found Russia's surveillance framework as falling short of adequate safeguards and therefore violative of art 8 of the European Convention on Human Rights (ECHR). This provision in the ECHR provided every individual the right to respect for one's "*private and family life, his home and his correspondence*".

[53] ibid.

[54] *Zakharov* (n 52).

[55] *Zakharov* (n 52).

communications of all users.[56] The ECJ reasoned that this generality of surveillance power made it even more important for the domestic law to provide a robust mechanism of review and supervision of its exercise. In its absence, the Russian domestic law would violate Article 8. Employing this heightened yardstick, the ECJ found that the system of prosecutorial supervision envisioned in Russia fell short of ECHR requirements as prosecutors were not independent enough in their functioning from executive control. The ECJ also found to be problematic the fact that the direct access system did not maintain any logs or records of interception, thereby rendering it difficult to evaluate whether interceptions were indiscriminately undertaken to advance legally untenable purposes. This decision was relied on along with others from the ECJ,[57] the European Court of Human Rights,[58] and the German Federal Constitutional Court,[59] all of which considered mass surveillance programs to be overly broad and capable of causing fear in the minds of citizens that they were under constant monitoring by the State. In fact, all these verdicts appear to consider the certainty of information under State control as being better than State authorities possibly holding voluminous information about an individual, and without one being able to ascertain this fact for sure.

These cases focused considerably on the structural and architectural aspects of the respective surveillance programs under challenge in each of them. But the Supreme Court's response in the *Aadhaar* verdict to the contentions built on these decisions was qualitatively different from the very essence of the judicial reasoning employed in them. The court's response can, at best, be characterised a narrow balancing exercise between immediate individual harms and social goals. During this exercise, the majority held that authentication records and 'authentication transaction data' can only be retained for a six-month period and must be deleted thereafter unless there is a judicial order authorising prolonged data retention.[60] It also limited the metadata that may be gathered to "*process metadata*" that helps identify when and where authentication may have taken place for purposes of subsequent dispute resolution and not any other categories of metadata that indicates the purpose served by such authentication and other transaction

---

[56] Ministry of Communications Order No. 70, issued on 20 April 1999.

[57] *Maximillian Schrems v Data Protection Commr* 2016 QB 527; *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* 2015 QB 127: (2014) 3 WLR 1607; *Tele 2 Sverige AB v Post-ochtelestyrelsen* 2017 QB 771: (2017) 2 WLR 1289.

[58] *Szabó and Vissy v Hungary* 2016 ECHR 579.

[59] *Proceedings on the Constitutional Complaints Against §§ 113a and 113b of the Telecommunications Act* (2010) judgment in 1 BvR 256/08 & Ors (BVerfG).

[60] *Aadhaar verdict* (n 19) 351.

details.[61] While not a point directly relating to surveillance, the majority ordered that the power to direct disclosure of Aadhaar data on grounds of national security be vested in a higher-ranking official than the joint secretary level specified in Section 33(2) of the Act.[62] In other situations of data disclosure, the court vested the data subject with a right to be heard by the district court sanctioning such disclosure.[63] It also extended the right to data subjects to directly raise grievances against data leakages and other offences, rather than rely on UIDAI and its authorised officers as stipulated in Section 47.[64]

While these may be considered quick fixes for any immediate harms that the court saw as arising from the workings of Aadhaar, they hardly address the long-term consequences of SRDHs and other potential applications of Aadhaar for big data analytics and profiling. In fact, the majority chose to not reference SRDHs despite the petitioners pointing out that when combined with multiple databases, the view that these data hubs offer about a citizen could be extremely potent. The majority observed that the averment of a "*surveillance state created by the Aadhaar project is not well founded, and in any case, taken care of by the diffluence exercise carried out with the striking down of certain offending provisions in their present form*."[65] There are significant strands in the majority's reasoning when dealing with surveillance that endorse the State's position based on the UIDAI's submissions that it has strengthened the security systems in place to avoid data leaks. This is particularly disconcerting because secure systems simultaneously double up as extremely sophisticated surveillance machineries. Instead, the majority would have done well to follow the various European court decisions that consistently opposed state-of-the-art mass surveillance architectures because their long-term consequences, while not fully ascertainable, made them even more worrisome and intrusive. But to do so, the majority should have appreciated, at both conceptual and factual levels, the distinc-

---

[61] *Aadhaar verdict* (n 19) 350.

[62] *Aadhaar verdict* (n 19) 423.

[63] *Aadhaar verdict* (n 19) 420-21.

[64] *Aadhaar verdict* (n 19) 424. It needs special mention here that many of these 'directives' are expressed as options and preferences for the State rather than mandatory orders. For instance, the majority *hopes* that "*if considered fit*," s 47 would be amended. Similarly, it concludes that a judicial officer may *preferably* function alongside a high-ranking bureaucrat to direct disclosure of Aadhaar data under s 33(2). As seen with the recent Aadhaar (Amendment) Ordinance 2019, the State has conveniently handpicked some of these options while ignoring the rest. *See*, Madhav Khosla and Ananth Padmanabhan, 'What the Aadhaar Amendment Bill Fails to Address' (*ThePrint*, 7 January 2019) <https://theprint.in/opinion/what-the-aadhaar-amendment-bill-fails-to-address/173958/> accessed 19 June 2019.

[65] *Aadhaar verdict* (n 19) 359.

tion between surveillance exceptions and surveillance-by-design. *PUCL* and other previous instances concerned the former, but the *Aadhaar* challenge demanded understanding the latter. The majority failed to draw this distinction, thereby applying a reasoning frame that was flawed to begin with.

IV. In Conclusion: The Need for More Robust Review

Behemoth adventures like the Aadhaar project spring up from a strong idea of technology solutionism. To its proponents and supporters, many of whom are senior bureaucrats and prominent business leaders, the biometric solution can be waved seamlessly like a magic wand to cure the State of all its ills. To some extent, the biometric solution may work in weeding out duplicate identities and fraudulent practices. However, the metrics put forth – the scale and pace of enrolment, the low cost per identity, the savings to the public exchequer – all pale when juxtaposed against the normative problems highlighted here. As experiences with the on-the-ground rollout of the Aadhaar project reveal, there have been leaks galore and misuse of Aadhaar data by both private and public entities within a limited period.[66] While no technical solution is ever fool-proof, any identity linked with such vast and varied facets of an individual's life are bound to elevate the cause for consternation. In a datafied world, vesting a significant number of personal data points within State custody is a recipe for abuse and potential profiling disasters. It also lowers, in a structural sense, the baseline of privacy protection that citizens must necessarily have against the State.[67]

This aspect is reflected in Justice Chandrachud's dissent in the *Aadhaar* case. Unlike the majority, he accounts for the structural reality that post-Aadhaar interactions between citizens and the State shall never be the same as in the pre-Aadhaar era. In a fine example of inductive reasoning, the dissent begins this exploration from what lies at the core of this project

---

[66] Srinivas Kodali, 'Forensic Probe Into Aadhaar Data Controversy in Andhra Pradesh Raises Troubling Questions' (*TheWire*, 15 April 2019) <https://thewire.in/government/andhra-pradesh-stolen-aadhaar-data> accessed 19 June 2019; Apoorva Mandhani, 'Prof. Shamnad Basheer Moves Delhi HC Against Aadhaar Data Leak; Demands Exemplary Damages' (*LiveLaw*, 18 May 2018) <https://www.livelaw.in/prof-shamnad-basheer-moves-delhi-hc-against-aadhaar-data-leak-demands-exemplary-damages/> accessed 19 June 2019.

[67] Whitley (n 34). Here, the authors argue that modern identity policy involves a complex socio-technical system that relies intensely upon technology while also altering the relationship between the individual and the State. Thus, choices such as biometric identities, use of a single identification number across government and the private sector, and an 'audit trail' that records details of every instance when an identity is verified against information stored on the register, can qualify as surveillance-by-design because of the extensive collection and use of personal information being proposed, as well as the expansive purposes for which the system would be used.

– biometric technology.[68] He notes that the deployment of this technology eradicates features such as anonymity and "*privacy by obscurity*" which, though not always desirable, bring some balance to the power dynamic between State and citizens.[69] He also rightly observes that this technology architecture, once compromised, cannot be secured again precisely because of the unique biometric features that make the project valuable in the first place.[70] This part of the discussion, and the impact of biometric solutions on privacy and exclusion as discussed in the dissent, are outside the scope of this article. Yet, they reveal a judicial approach that assesses the technology design in a deeper way than the majority did.

Proceeding further, the dissent assesses the overall technology solution to be legally disproportionate because "*an entire population cannot be presumed to be siphoning huge sums of money in welfare schemes or viewed through the lens of criminality, and therefore, considered as having a diminished expectation of privacy.*"[71] Justice Chandrachud examines the authentication architecture from the time biometric information is captured at point-of-sale devices, to conclude that extensive authentication transaction data vests with the UIDAI. This fact, coupled with the lack of transparency and inadequate grievance redressal mechanisms, "*exacerbate the overall risk associated with data retention*," including potential surveillance activities using the Aadhaar database.[72] Third parties can access biometric authentication information, link it with other information, and erode the personal control that an individual has over her information – a systemic harm arising from big data applications.[73] He also underscores the profiling risks in making Aadhaar numbers the "*central unifying feature that connects the cell phone with geo-location data, one's presence and movement with a bank account and income tax returns, food and lifestyle consumption with medical records*," thereby starting a "*causal link between information which was usually unconnected and was considered trivial.*"[74] This opinion, which conclusively shuts down the project, has been recently followed by

---

[68] *Aadhaar verdict* (n 19) 763.
[69] *Aadhaar verdict* (n 19) 767.
[70] *Aadhaar verdict* (n 19) 768-69.
[71] *Aadhaar verdict* (n 19) 835.
[72] *Aadhaar verdict* (n 19) 936.
[73] *Aadhaar verdict* (n 19) 845. Justice Chandrachud factually substantiates this point by exploring the contractual arrangement between UIDAI and the private vendor that licensed the biometric storage solutions software, and concluding that the vendor was given unfettered access to the Aadhaar database.
[74] *Aadhaar verdict* (n 19) 854, 856. Subsequently, the dissent notes: "*When Aadhaar is seeded into every database, it becomes a bridge across discreet data silos, which allows anyone with access to this information to reconstruct a profile of an individual's life. It must be noted while s. 2(k) of the Aadhaar Act excludes storage of individual information related*

the Jamaican Supreme Court in *Julian Robinson* v. *Attorney General of Jamaica*[75] to invalidate the national identification and registration statute.

To conclude, the majority verdict in *Aadhaar* ought to have developed a test along the lines of the 'chilling effects doctrine' to evaluate the long-term harms of the project rather than confine its enquiry to the immediate harms and solutions associated with such architectures. It should also have developed sounder judicial models for assessing technological design and structural features against the optimal privacy baseline in a democratic society. As we showed earlier, part of the majority's failure to do so can be attributed to the long history of privacy jurisprudence in India that evolved in the context of such balancing between immediate harms and larger social goals. But we still cannot ignore the fact that the court had received considerable instruction from the bar through judicial precedents and scholarship that tackled similar concerns arising from architectural interventions. Shyam Divan and other counsel appearing for various petitioners had relied on the idea of limited government, one that went beyond individual harms as narrowly framed to a more structural sense of what the power balance between the State and the citizen ought to be for democracy to survive. The majority chose not to address these submissions in an appealing manner, instead taking an easier route of reading in procedural safeguards. Through this choice, the majority let go of a valuable opportunity to engage with the kind of long-term harms and structural imbalances that any democratic society must be prepared to confront in the age of emerging technologies and big data analytics.

---

to race, religion, caste, tribe, ethnicity, language, income or medical history into CIDR, the mandatory linking of Aadhaar with various schemes allows the same result in effect."

[75] 2019 JMFC Full 04. *See*, Madhav Khosla and Ananth Padmanabhan, 'How Jamaican Supreme Court has Killed India's Hope of Selling Aadhaar to the World, for Now' (*ThePrint*, 22 June 2019) <https://theprint.in/opinion/how-jamaican-supreme-court-has-killed-indias-hope-of-selling-aadhaar-to-the-world-for-now/252199/> accessed 19 June 2019; Gautam Bhatia, 'The Afterlife of the Aadhaar Dissent: The Jamaican Supreme Court Judgment Quashing NCID' (*LiveLaw*, 14 April 2019) <https://www.livelaw.in/columns/jamaican-sc-national-biometric-identification-system-144269> accessed 19 June 2019.