
INFRASTRUCTURAL CONSENT: RESIDENTIAL SURVEILLANCE AND THE COHERENCE OF CONSENT UNDER THE DPDPA 2023

Jayesh Nitharwal, OP Jindal Global University

ABSTRACT

Residential management platforms such as MyGate have become default infrastructure across urban Indian housing societies, conditioning occupancy on enrolment in systems that render the daily life of the home into a continuous behavioural record. This paper asks whether the consent obtained at that residential threshold, as a condition of tenancy, can satisfy the requirement of free, specific, informed, and revocable consent that Section 6 of the Digital Personal Data Protection Act 2023 demands.

Through doctrinal analysis anchored in a single-site study of MyGate within the Mumbai housing market, it argues that the consent fails each statutory criterion simultaneously and for one structural reason. It is not free, because refusal entails the loss of the home in a saturated market that offers no genuine alternative; it is neither specific nor informed, because data surrendered for security migrates to behavioural profiling across a contextual boundary the resident never authorised; and it is not revocable, because the processing is a continuing relationship the architecture is built to make irreversible.

The paper locates the common cause in what it terms infrastructural consent, consent extracted as the condition of a necessity the person cannot, on the statute's own criteria exit, which the notice-and-consent framework was never designed to govern. Drawing together the Srikrishna Committee's no-bundling rule, the continuing-consent doctrine of *Samira Kohli*, contextual-integrity theory, and the natural-rights structure of privacy in *Puttaswamy*, it proposes the Residential Consent Doctrine as the framework Indian private law already contains for the problem it has not yet named.

Keywords: data protection; consent; residential surveillance; Digital Personal Data Protection Act 2023; surveillance capitalism; privacy; contextual integrity.

I am deeply grateful to Tara Bhattacharya Gupta, whose early collaboration and generous engagement helped shape this project in its formative stages. Her insight into the questions of privacy and the home animates much of what follows, and I remain thankful for her friendship and encouragement throughout. However, the errors are all mine.

PART I — INTRODUCTION

1.1 The Threshold of the Home

There is an old order of priorities in Indian life, recited so often it has worn smooth. *Roti, kapda, aur makaan*.¹ Food, clothing, and shelter. The *makaan* sits at the end of that list not because it matters least but because it contains the others. It is the place to which food is brought and within which a life is assembled. Law has always understood this. Across contract, property, and constitutional doctrine, the home is treated as the paradigmatic private domain, the space a person is entitled to occupy without justification to anyone, the last interior that the rest of the world may not enter without leave. The tenant who signs a lease secures, at minimum, the quiet enjoyment of that interior. She secures the right to come and go, to receive whom she chooses, to live unobserved.

Consider, then, what now stands at the entrance to that interior. To enter many urban Indian housing societies today, a resident opens an application on her phone. To admit a visitor, she approves a request that records the visitor's name, photograph, phone number, and purpose. Her own entries and exits are timestamped, her vehicle's departure generates a notification, the domestic workers she employs are logged in and out against her account, and the patterns of her week accumulate in a database she does not control and cannot inspect. When she leaves, when she returns, who comes to her door, how often. The platform that performs these functions is marketed as a security and convenience solution, and at the threshold it behaves like one. But the threshold is also where the data is taken. The same gate that promises safety operates, in the same motion, as a checkpoint of extraction. The home as sanctuary and the home as surveilled threshold are no longer separable spaces. They have become the same address.

This is not a marginal inconvenience affecting a handful of premium developments. Residential management platforms, with MyGate foremost among them and NoBrokerHood, ApnaComplex, and ADDA close behind, have moved in less than a decade from pandemic-era novelty to default infrastructure across metropolitan housing societies. Their spread matters for two reasons that the law has not yet reckoned with together. The first is scale. As these platforms approach saturation in cities like Mumbai, enrolment ceases to be a feature a resident selects and becomes a condition of occupancy she cannot decline. The second is the nature of

¹ *Roti Kapada Aur Makaan* (Manoj Kumar Productions 1974) directed by Manoj Kumar.

what is collected. Residential movement data, meaning who enters a home, when, accompanied by whom, and in what rhythm, is among the most intimate information a person generates, precisely because it is generated at the site the law has always held most private. The significance of the problem is therefore not exhausted by the familiar vocabulary of data breaches or privacy anxiety. It reaches a more structural question, which is whether the legal mechanism India has chosen to govern this extraction can do the work the law assigns to it. That mechanism is consent.

1.2 Background: Consent as the Organising Principle

The Digital Personal Data Protection Act, 2023, like the comparative regimes it draws upon, makes consent the central ground on which the processing of personal data is rendered lawful.² Section 6 requires that consent be free, specific, informed, unconditional, and unambiguous, given through a clear affirmative action, and it requires further that consent be capable of withdrawal.³ The structure mirrors the consent-centred reorientation that Indian law has pursued across other domains over the past decade, in which status, presumption, and inferred acquiescence are displaced by an affirmative and evaluative inquiry into whether the person actually agreed. Consent, on this design, is the threshold that separates lawful processing from violation, just as in other consent-based regimes it separates the permitted from the prohibited. The legitimacy of the entire framework rests on the assumption that this threshold is real, that the consent the statute requires is consent the conditions of collection can actually produce.

1.3 The Problem and the Gap

The difficulty is that residential surveillance platforms operate on consent obtained at the single moment of enrolment, and that enrolment is, in practice, mandatory as a condition of tenancy. This produces a tension that existing scholarship has not confronted on its own terms. The Indian literature has examined the weaknesses of the DPDPA extensively, including its government exemptions, its omission of a right to be forgotten, and the structural inadequacy of its consent mechanism, and the surveillance-capitalism scholarship has supplied a powerful account of why consent functions, in extractive systems, as a shield for the extractor rather than

² Digital Personal Data Protection Act 2023, s 4

³ Digital Personal Data Protection Act 2023, s 6(1) (setting out the criteria of free, specific, informed, unconditional and unambiguous consent) and s 6(4) (right to withdraw with ease comparable to that with which consent was given).

a constraint upon him. The constitutional scholarship around *Puttaswamy* has established privacy as a fundamental right governed by a demanding proportionality framework.⁴

What none of this work has done is bring these threads to bear on the specific question of residential surveillance consent, namely whether the consent extracted at the residential threshold, as a condition of housing, can satisfy the criteria the DPDPA itself lays down. The tendency has been to treat the consent defect as a problem of enforcement or disclosure, a procedural shortfall to be corrected by better notices and clearer dashboards. What remains insufficiently examined is whether the consent obtained in this setting fails not procedurally but structurally, whether the conditions of residential enrolment make free, specific, informed, and revocable consent not merely difficult to obtain but conceptually impossible to obtain. It is this question of internal doctrinal consistency that frames the inquiry undertaken here.

Research Question: Does mandatory enrolment in residential surveillance platforms as a condition of tenancy constitute free, specific, informed, and revocable consent under Indian contract and data protection law?

1.4 Sub-Questions and Working Hypothesis

This central inquiry resolves into four subsidiary questions, each tracking one of the statutory criteria the law requires consent to satisfy. The first asks whether consent can be free when refusal carries the loss of housing and the residential market offers no realistic alternative. The second asks whether consent can be specific when a single enrolment authorises a bundle of categorically distinct processing operations, from entry management to behavioural profiling to third-party transfer to financial integration, that belong to incompatible informational contexts. The third asks whether consent can be informed when the operations to which a resident agrees are, by design, opaque to her comprehension. The fourth asks whether consent can be revocable when withdrawal is structurally foreclosed by the conditioning of tenancy on continued enrolment.

The working hypothesis is that the consent obtained through residential surveillance enrolment is not an isolated irregularity in an otherwise functioning framework but an expression of a deeper structural failure. Once consent can be extracted as a condition of a basic necessity, bundled across incompatible purposes, sustained on opacity, and rendered practically

⁴ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

irrevocable, its role as the organising criterion of lawful processing collapses in this context. The enrolment does not merely strain the four statutory criteria. It fails each of them at once, and the simultaneity is not coincidental. It points to a common structural root that the paper identifies in its later analysis.

1.7 Aim and Objective

The objective of this study is not to argue that residential surveillance is undesirable as a matter of policy, nor to mount a constitutional challenge to any platform's operations, since a separate constitutional inquiry lies beyond this paper's frame. The aim is narrower and doctrinal. It is to examine the internal logic of consent as it operates in the residential surveillance context, and to assess whether a consent-based legal framework can remain coherent while treating consent as both the foundational requirement for lawful data processing and a formality satisfiable by enrolment conditioned on housing. The paper treats data protection law as a doctrinal system whose legitimacy depends on the consistent operation of its organising principle. Where that principle is affirmed in statute but suspended in application, the system does not merely leave a category of persons unprotected. It becomes conceptually unstable. The study's contribution is to name that instability precisely and, on the strength of that diagnosis, to propose a doctrinal framework adequate to it, which the paper calls the Residential Consent Doctrine.

1.8 Scope and Delimitations

The analysis is situated within Indian private law, meaning contract and data protection, in the period following the enactment of the DPDPA, 2023,⁵ and is anchored empirically in the residential housing market of Mumbai, whose acute unaffordability and dense vertical development make it the clearest site at which the structural conditions under examination obtain. MyGate is treated as the primary case study, both as the dominant platform in this space and as a representative instance of the broader category of residential surveillance infrastructure.

The inquiry is confined to the coherence of consent within private law and does not undertake an empirical assessment of the prevalence of these platforms, the security outcomes they produce, or the enforcement record of the Data Protection Board. Constitutional materials,

⁵ Digital Personal Data Protection Act 2023.

including the several opinions in *Puttaswamy*,⁶ the positive-obligation jurisprudence, and the proportionality framework, are engaged only where they illuminate why the private-law consent fails, and not as independent grounds of constitutional invalidity, since the constitutional argument proper is reserved for separate treatment. Comparative materials, principally the GDPR and the guidance of the European Data Protection Board, are drawn upon only where they clarify the doctrinal structure of the consent criteria rather than as authorities to be transplanted wholesale.

1.9 Roadmap

The argument proceeds as follows. Part II synthesises the scholarly conversation across four registers, namely the genealogy of surveillance power, the political economy of extraction, the Indian constitutional discourse around privacy, and the Indian data-protection literature, and locates within it the gap this paper addresses. Part III sets out the doctrinal methodology, the basis for site and case selection, and the study's limitations. Part IV, the analytical core, establishes the architecture of residential surveillance as the factual predicate and then works through the consent failures in turn, taking the free criterion first, then the specific and informed criteria together, then the revocable criterion, before drawing them together to show that they share a single structural root and answering the principal objections the argument invites. Part VI also states the Residential Consent Doctrine that follows from the analysis, anchors it in existing doctrinal and comparative materials so that it reads as development rather than invention, and concludes by returning to the threshold of the home with which the inquiry began.

PART II — LITERATURE REVIEW

The literature assembled for this paper was identified through a thematically layered search that moved from the specific statutory and doctrinal vocabulary of the field toward its broader theoretical foundations. Search terms ranged from the narrow and provision-specific, including DPDPA Section 6, free consent, no-bundling, residential surveillance, and MyGate, to the conceptual and theoretical, including surveillance capitalism, behavioural surplus, contextual integrity, informational self-determination, and the Hohfeldian analysis of rights.

⁶ *Justice K S Puttaswamy (Retd.) v Union of India* (n 4).

The review draws on several categories of source. It engages primary legal materials, including the DPDPA, the Indian Contract Act, the report of the Justice Srikrishna Committee, and the several opinions in *Puttaswamy*. It engages peer-reviewed and institutional scholarship on Indian data protection, including the work of Bailey, Parsheera, Bhandari, and the analyses produced by the Vidhi Centre for Legal Policy and allied bodies. It engages the foundational theoretical literature on surveillance and extraction, principally Foucault, Deleuze, Varoufakis, and Zuboff. It engages the theoretical apparatus of contextual integrity and natural rights through Nissenbaum and Finnis. And it engages investigative and case-study material on the conduct of residential platforms, principally the reporting of Kodali.

Sources were included where they contributed to understanding how consent is constructed, how it is displaced, or why residential data collection escapes the protection the law nominally provides, and were set aside where their orientation was purely empirical, journalistic, or advocacy-driven without sustained engagement with the doctrinal or theoretical questions at issue. The emphasis throughout fell on interpretive relevance rather than descriptive breadth, so that the review remains organised around the structural question the paper pursues rather than around a catalogue of the field.

2.1 The Genealogy of Surveillance and the Production of the Dividual

The scholarship on surveillance does not speak with one voice, and the most productive way into it is through a disagreement its authors never quite stage among themselves but which their work, read together, forces into the open. The question is what surveillance does to the person it observes, and the answers move across half a century from the disciplinary to the economic, each author inheriting the previous one's insight and turning it toward a problem the previous one could not see.

Foucault supplies the inheritance the others build upon. His account detaches surveillance from the act of watching and attaches it to a structural effect, the production of a subject who, uncertain whether she is observed at any given moment, regulates herself as though she always were. The mechanism does not require a watcher who is present, only a watcher who might be, and its product is conduct shaped in anticipation of a gaze that can never be confirmed.⁷

⁷ Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan tr, Penguin 1977) 201.

This is the foundational move on which everything later depends, the recognition that surveillance is productive rather than merely observational, that it makes the watched into something she would not otherwise have been. What Foucault's account does not yet contain, because the technology that would demand it did not yet exist, is any sense that this self-regulating subject might also be decomposed, that she might be broken into parts and reassembled elsewhere.

Deleuze supplies exactly that, and in doing so marks the break that separates the disciplinary world from the present one. His brief and deliberately compressed account distinguishes the societies of discipline Foucault described, which operated through enclosed institutions that produced finished individuals, from the societies of control, which operate through continuous modulation that never finishes its subject. The person who emerges, or rather who is dissolved, is no longer an individual at all but what Deleuze names the "dividual," a being decomposed into data to be processed by systems that never meet her as a whole.⁸

The dividual is the conceptual hinge of this entire paper, because it identifies with precision what a residential platform does to a resident, and the literature that follows can be read as an extended argument about why the dividual is produced and to whose benefit. Deleuze himself does not answer that question. His modulation is control as an ambient condition, an atmosphere rather than an enterprise, and it leaves unexplained why anyone would build the machinery of decomposition in the first place.

McMullan and Ian Alan Paul carry the disciplinary account toward the digital without yet resolving that question of purpose. McMullan tests whether the panopticon survives its own digitization and finds that its core mechanism, behavioural modification through perceived observation, not only survives but intensifies once the watcher becomes algorithmic and the architecture dissolves into dispersed sensors.⁹ Paul presses the identification further, collapsing the apparent distance between the prison and the computer by showing that both run on a single logic of capture, classification, and behavioural modification, so that control reveals itself as discipline automated and accelerated.¹⁰

⁸ Gilles Deleuze, 'Postscript on the Societies of Control' (1992) 59 October 3, 5.

⁹ Thomas McMullan, 'What Does the Panopticon Mean in the Age of Digital Surveillance?' *The Guardian* (London, 23 July 2015).

¹⁰ Ian Alan Paul, 'Are Prisons Computers?' (*ianalanpaul.com*) <https://www.ianalanpaul.com> accessed 25 June 2026, 5.

These authors agree on the essential and now well-established point, that surveillance produces its subject rather than merely recording her, and their disagreements are generational and methodological rather than substantive, Foucault reading the archive, Deleuze writing diagnosis, Paul writing provocation. What none of them supplies, because it falls outside the frame each constructed, is the economic engine that drives the decomposition they describe. The genealogy establishes the mechanism of surveillance and its effect upon the subject with great force, and stops precisely where the question of profit begins. It is at that boundary that the next body of literature takes up the conversation, and it is there that the decomposition Deleuze named acquires the purpose he declined to give it.

2.2 The Political Economy of Extraction and the Legitimizing Work of Consent

The political-economy literature begins where the genealogy ends, by supplying the purpose the decomposition serves, and here too the field is organised around a disagreement that the residential context will later resolve. Varoufakis and Zuboff agree that human experience is now the raw material of an extractive economy and divide over what to call the system that extracts it, and the division is worth holding onto because each author sees something the other's frame obscures.

Varoufakis names the system technofeudalism and insists it has passed beyond capitalism altogether. Capital's commanding power, on his account, is not intrinsic to the machinery but produced by enclosure, by the prior dispossession of any alternative, and what reproduces it is the unpaid labour of those he calls cloud serfs, the platform users who generate value simply by living within the system that records them.

The frame is useful for the residential setting because it names the resident's position with uncomfortable accuracy. The resident who logs her visitors and approves her entries performs precisely the unpaid productive labour Varoufakis describes, generating the behavioural record on which the platform's value rests, inside a fief she occupies but does not own and from which she cannot meaningfully exit.¹¹ What Varoufakis's frame does less well is specify the legal mechanism through which the extraction is made to appear authorised, because his quarrel is with the structure of the economy rather than with the instruments of its law.

¹¹ Yanis Varoufakis, *Technofeudalism: What Killed Capitalism* (Bodley Head 2023) 3.

Zuboff supplies that mechanism, and her account is the one this paper relies upon most heavily, because she alone tracks the extraction down to the legal instrument that legitimates it. Her central claim is that surveillance capitalism "unilaterally claims human experience as free raw material for translation into behavioural data,"¹² which it refines into prediction products and trades in markets for future behaviour. Three of her findings carry directly into the residential analysis.

The first concerns the position of the person extracted from, who is, in her precise formulation, neither customer nor worker nor product but the raw-material supplier, the source of a surplus harvested for the benefit of others who stand downstream as the actual customers.¹³ The second is her insistence, against the comfortable language of privacy erosion, that privacy is "not eroded but redistributed," that the right to decide what is disclosed is taken from the person and concentrated in the firm,¹⁴ a reframing that converts the residential problem from one of lost privacy into one of seized decision rights.

The third is her direct engagement with consent, drawn through the contract scholarship of Radin and Kim, in which the terms-of-service agreement becomes a "private eminent domain," a unilateral seizure in which the sacred notions of agreement and promise devolve into a "talismanic" signal that the firm wishes the recipient to be bound.¹⁵ Zuboff records the empirical hollowing of that consent in the calculation that reading the privacy policies one ordinarily encounters in a year would consume seventy-six working days, a figure that converts the fiction of informed agreement from an abstraction into an arithmetic certainty.¹⁶

The convergence between the two authors matters more for this paper than their quarrel, and it is the residential platform that makes the convergence visible. Where Varoufakis sees a serf generating value by existing and Zuboff sees a supplier furnishing surplus by being rendered into data, the MyGate resident is demonstrably both, and the decomposition Deleuze named in the previous section is now explained, because the dividual is produced for the reason Zuboff identifies, that the fragments are saleable, and inside the enclosure Varoufakis describes, from

¹² Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 8.

¹³ *ibid* 10.

¹⁴ *ibid* 10, 48.

¹⁵ *ibid* 48–49.

¹⁶ *ibid* 49.

which there is no exit. The decomposition is modulation for sale, and the consent obtained at the threshold is the instrument that makes the sale appear consented to.

This is the load-bearing insight the paper carries into its doctrinal core, that consent in these systems does not constrain extraction but authorises it, that it is the legal device through which a taking is dressed as an agreement. Zuboff records the residential case directly, observing of the landlord who conditions tenancy on a prospective tenant's social-media access that it is those "with the least resources and the fewest options" who are trapped in a bargain where privacy is the price of participation.¹⁷ It is that observation, lifted out of her account and set down in the Indian housing market, that the discussion takes up when it turns to whether a consent so extracted can be called free.

The political economy establishes that consent legitimates rather than constrains. It does not, because it operates at the altitude of systems, descend to the statutory criteria of any jurisdiction and show the legitimisation failing criterion by criterion, and that descent, into Section 6 of the DPDPA and the rule the Srikrishna Committee built to prevent exactly this bargain, is where the Indian literature resumes the conversation.

2.3 Contextual Integrity and the Limits of Consent as an Information-Flow Rule

The genealogy established that surveillance produces its subject and the political economy established that it does so to extract a saleable surplus, but neither tells us when a particular flow of information is wrongful, and it is that question the third body of literature answers. Nissenbaum's contribution is to relocate the wrong of surveillance away from secrecy and toward flow, and the relocation is what makes her framework indispensable rather than merely adjacent to the argument.

Privacy, on her account, is not the concealment of information but the maintenance of "contextual integrity," the set of norms governing how information properly moves within the context in which it was generated.¹⁸ A violation occurs not when information is known but when it travels from the context of its origin into a context whose norms forbid its arrival.¹⁹ Information disclosed to a physician is not thereby available to an employer, and the wrong of

¹⁷ *ibid* 174.

¹⁸ Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 101, 119.

¹⁹ *ibid* 119-20, 125.

the second flow is not that the information was secret but that it crossed a boundary the original context did not authorise it to cross.

The decisive feature of this account, for a paper about consent, is that it locates the wrong at a level individual agreement cannot reach. The norms of a context are not the individual's to waive, because they are the shared expectations that constitute the context itself, which means a person cannot consent her way out of a contextual-integrity violation any more than she can authorise her physician to disclose her records to her insurer by signing a form that purports to permit it.

This is the point at which Nissenbaum's framework and the Indian constitutional record meet, because Chandrachud, writing for plurality in *Puttaswamy*, reasoned his way to the same destination without the vocabulary, holding that information surrendered in one relationship cannot legitimately be redirected to another without consent specific to that redirection.²⁰ The convergence is useful precisely because it is unplanned. An American theorist building a framework from first principles and an Indian judge reasoning from constitutional privacy arrive at the same structural claim, that the legitimacy of an information flow is governed by the context of disclosure and not by the bare fact of agreement, and the agreement between them lends the principle a weight neither source carries alone.

The framework also answers the objection it is most likely to face, and the answer matters enough to the later argument to be established here. A platform of the MyGate type will say that the contextual norm of the gated community has simply shifted, that residents now expect digital access management and that ubiquity has remade the baseline of reasonable expectation. The contextual-integrity literature rejects this move on principle, holding that a technological practice cannot validate itself by the fact of its own spread, that the mere prevalence of a departure from a norm does not convert the departure into the new norm, and that legitimate normative change requires deliberation rather than the accomplished fact of deployment.

The burden lies on the departing practice to show that its departure serves a value sufficient to outweigh the privacy it costs, and convenience and efficiency are not such values, they are the preferences the framework already distinguishes from the values capable of justifying a new flow. What the literature supplies, then, is not merely a description of the wrong but a rule for

²⁰ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 306-310 (Chandrachud J).

adjudicating it, one that survives the saturation defence the residential platform will raise. It does not, however, specify how that rule engages a particular statutory criterion, and the criterion it most directly informs, the requirement that consent be specific to a defined purpose, is one the Indian data-protection literature was built to interpret.

2.4 The Indian Data-Protection Conversation and the Engineering of Consent's Failure

The Indian literature converges, from several directions and across a decade of legislative development, on a single finding that the scholarship states more plainly than any single author intends, that the consent mechanism is known to be structurally inadequate and was weakened in the very process of its enactment. The Srikrishna Committee report is the indispensable source, because it preserves the design the framework was meant to carry before that design was diluted, and it states the operative principle the residential platform offends.

The Committee was explicit that consent operates in practice as an all-or-nothing formality that is routinely uninformed, and it answered that diagnosis with a rule that is, for the purposes of this paper, the single most important provision in the entire consent chapter, the requirement that consent cannot be made a condition of access to a service unless the processing consented to is strictly necessary for that service.²¹ This no-bundling rule is the direct legislative ancestor of the free-consent requirement, and it was drafted to forbid precisely the bargain in which access is conditioned on agreement to processing the service does not need, which is the bargain residential enrolment embodies.

The Committee grounded the rule, moreover, in a conception of autonomy that is relational and public rather than atomistic, treating individual control over data not as a private preference to be traded but as a structural condition of self-determination, so that its violation injures not merely a person's wishes but the conditions under which she can be self-governing at all.

The scholarship that follows the Act traces how exposed the residential context remains once that design was diluted in passage. Kodali documents that access-management and biometric systems of exactly the MyGate type continue to proliferate, and identifies the mechanism by which they may escape regulation entirely, the exemption power the Act confers on the executive, which could place residential platforms outside the statute's requirements by

²¹ Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) 34.

notification, without parliamentary ratification and without stated criteria, so that whatever consent protections the framework offers residents are, in his account, revocable at the executive's discretion.²²

Bailey and Sane, examining the regulation of non-personal data in India, establish that the boundary between personal and non-personal data cannot be drawn in a strictly binary way. The same data, they argue, may be personal when processed by one party and non-personal when processed by another, anonymised data may be re-identified and must then be treated as personal once more, and whether data is personal cannot be settled by its provenance alone. The instability bears directly on the residential case, because a platform may characterise the aggregate record of entries and exits as anonymised non-personal data falling outside the consent regime, and if that characterisation held it would place the most revealing product of the surveillance beyond the reach of the framework meant to govern it.²³

The most directly usable contribution comes from Srivastava and Chaudhari, who, writing on data portability under the draft framework that preceded the Act, ground the defect in the doctrine of privity of contract. Consent, they argue, establishes a direct contractual relationship between the data principal and the fiduciary, and where one person ports data that carries information about a second person, that second person is bound by a contract to which she was never party.²⁴ The secondary user has given no consent, has no visibility into the arrangement, and cannot withdraw an authorisation she never granted, which deprives her of a requirement the framework itself treats as fundamental to valid consent, the capacity to withdraw it.

The argument was made of the predecessor Bill, but the enacted Act reproduces the same consent-and-withdrawal structure on which it depends. The residential gate reproduces the same relational defect, since the resident's enrolment binds the visitor, the domestic worker, and the delivery rider whose data it captures and who never agreed to anything at all.

A recurring feature of this literature, and one the paper will exploit rather than merely note, is its reluctance to connect these findings to the surveillance-capitalism account that would

²² Srinivas Kodali, 'Ten Reasons Why the Digital Personal Data Protection Bill Won't Empower the Public' (*The Wire*, 7 August 2023) <https://thewire.in/law/will-the-data-protection-law-empower-the-public> accessed 3 July 2026.

²³ Rishab Bailey and Renuka Sane, 'Regulating "Non-Personal Data": Developments in India' in Bart Van Der Sloot and Sascha Van Schendel (eds), *The Boundaries of Data* (Amsterdam University Press 2024) 227, 241.

²⁴ Aparajita Srivastava and Nehaa Chaudhari, *Social Graph Portability* (Data Catalyst 2019) 5–7.

explain them, so that the authors diagnose the symptoms of a structurally inadequate consent regime while passing quickly over the extractive economic logic that produces the inadequacy, and in one instance accept the platform's characterisation of its inferred records as its own intellectual property without registering that the raw material was the user's behaviour and the processing merely the platform's appropriation of it.

The Indian literature thus supplies the statutory spine of the argument, the no-bundling rule and the language of relational defect in consent, and leaves open the question its own findings raise, why a framework so plainly inadequate to the residential case should nonetheless treat the consent it obtains as sufficient. That question cannot be answered from within data-protection doctrine alone, and the answer the paper gives draws on a theory of rights that explains why some intrusions lie beyond the reach of any consent the framework could obtain.

2.5 Natural Rights, the Structure of Immunity, and the Ceiling on Consent

The preceding literature establishes that residential consent fails the statute's criteria, but failure against a criterion invites the reply that a better-drafted consent would succeed, and to foreclose that reply the argument needs a source establishing that no consent obtained in this setting could succeed, because the right at stake is not the kind of thing this consent can waive. Finnis supplies the apparatus, and the two elements of his account that the paper relies upon are best taken in the order that builds the claim.

The first is his reconstruction of the relationship between natural and positive law, in which the principles that ground rights are recognised by positive law rather than created by it, so that a statute enjoys, in his image, the creative freedom of an architect working within constraints it did not author but cannot exhaust. The implication for the residential case is exact. A right that positive law recognises rather than confers cannot be exhausted by the instruments of positive law, which means a contractual term purporting to waive it operates on something the contract did not grant and therefore cannot, by its own authority, take away.²⁵

This is the philosophical foundation beneath Nariman's formulation in *Puttaswamy*, that privacy is recognised and not granted by the Constitution, and the two sources read together convert a constitutional dictum into a structural claim about what consent can and cannot do,

²⁵ John Finnis, *Natural Law and Natural Rights* (2nd edn, Oxford University Press 2011) 23–25.

that one cannot contractually surrender what one did not receive through contract in the first place.²⁶

The second element gives the claim its doctrinal edge, and it comes from Finnis's reconstruction of Hohfeld. Among the four relations Hohfeld distinguished, the one the residential case requires is the immunity, the position in which one party simply lacks the power to alter another's legal standing, so that the second party's right stands beyond the first party's reach regardless of what instruments the first deploys.²⁷

Construed as an immunity, the resident's privacy is not a liberty she trades or a claim she might be argued out of but a position the platform has no power to change, which means the defect in residential enrolment is not, at its deepest level, that the consent was unfree or unspecific or uninformed, though it was each of these, but that the platform never held the power to extract a valid waiver at all, because the right was structured as an immunity against exactly that exercise of power.

Finnis sharpens the same point through the distinction between rights one exercises and rights that protect against a specified wrong, the latter carrying a conclusory force that mere preference-rights lack, and the right not to have one's home rendered into a continuous behavioural record as the price of occupancy belongs to the second class, a protection against a defined wrong rather than a liberty whose exercise is open to negotiation.²⁸ This is the apparatus that converts the paper's many findings of consent-failure into a single structural claim, that consent was never the operative question, because the power to obtain it was absent from the start. What the natural-rights account does not by itself provide is the comparative and contractual scaffolding that shows the same ceiling operating inside positive law's own categories, and that scaffolding, drawn from the contract scholarship and the comparative consent standards, is the last body of literature the review assembles.

2.6 The Contractual and Comparative Architecture of Consent

The final body of literature returns the argument from the height of natural-rights theory to the ground of doctrine, and it does so because the paper's claims must be sustainable inside positive

²⁶ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1, 598, 601 (Nariman J).

²⁷ Finnis (n 25) 199–205.

²⁸ *ibid* 209–10.

law's own categories and not only above them. The contract scholarship that Zuboff imports, principally Radin and Kim, is the bridge, because it shows the consent failure operating as a matter of contract doctrine rather than political economy.

Radin's account of boilerplate as a form of private legislation, a unilateral imposition of terms that strips rights without the bargaining that contract presupposes, gives the residential enrolment its contractual name, a "private eminent domain" in which the resident is bound to a legal universe of the platform's devising as the condition of a transaction she cannot avoid.²⁹ Kim's analysis of the adhesive, take-it-or-leave-it structure of digital terms supplies the mechanism, the absence of any genuine assent beneath the formal click.³⁰ These authors establish that the defect the political economy described as extraction is, in the vocabulary of contract, a failure of the assent that contract requires, so that the consent residential enrolment obtains is defective not only against the data-protection statute but against the older private-law standard the statute presupposes.

The comparative material completes the scaffolding by showing that the standard the paper urges is not invented for the occasion but already operates in the regime the DPDPA was modelled upon. The European framework treats the conditioning of a service on consent to unnecessary processing as a defect of freedom rather than a mere irregularity, holding that consent bundled with access to a service the processing does not require cannot be regarded as freely given,³¹ and it treats a clear imbalance of power between the parties as a circumstance in which the freedom of consent is presumptively absent.³²

The convergence between this comparative standard and the Srikrishna Committee's no-bundling rule is the point the paper will press, because it shows the rule that residential enrolment violates to be neither a peculiarly Indian nicety nor a theorist's aspiration but a settled feature of the consent architecture across the regimes that take consent seriously, so that the platform's bargain fails not against one jurisdiction's idiosyncrasy but against the shared structure of consent doctrine itself.

²⁹ Margaret Jane Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press 2013) 15.

³⁰ Nancy S Kim, *Wrap Contracts: Foundations and Ramifications* (Oxford University Press 2013), as cited in Zuboff (n 12) 48.

³¹ Regulation (EU) 2016/679 (General Data Protection Regulation) (2016) OJ L119/1, art 7(4).

³² *ibid*, recital 43.

With the contractual name of the defect established and the comparative standard in place, the review has assembled every element the analysis requires, the mechanism of surveillance, the economic purpose of extraction, the contextual role that consent cannot override, the statutory ancestry of the no-bundling requirement, the natural-rights ceiling on what consent can waive, and the contractual and comparative architecture that holds the same ceiling inside positive law. What no source in the field has done is bring these elements to bear together on the residential threshold and ask whether the consent obtained there, as the price of a home, can satisfy the criteria the DPDPA itself lays down, and it is that assembled question the discussion now takes up, criterion by criterion, beginning with the architecture to which the resident is asked to consent.

PART III — METHODOLOGY

3.1 Research Design: Qualitative Doctrinal Method

This study adopted a qualitative doctrinal research design centred on the interpretive analysis of statutory texts, judicial opinions, committee reports, and theoretical scholarship bearing on consent and data protection in India. The inquiry was not empirical. Its object was the internal coherence of a legal doctrine, specifically whether consent can perform the work the Digital Personal Data Protection Act assigns to it once that consent is extracted at the residential threshold as a condition of tenancy. Questions of doctrinal consistency, conceptual stability, and the alignment of a statute's stated principle with its operation in a particular setting cannot be answered through quantitative measurement. They require the close reading of legal texts and the evaluation of how legal principles hold or fail when applied to a concrete fact pattern.

The approach was qualitative in a second sense, engaging theoretical scholarship on consent, surveillance, autonomy, and the structure of legal rights not as independent sites of debate but as interpretive instruments brought to bear on Indian statutory and constitutional material. The method remained analytical rather than normative throughout. The objective was not to advocate that residential surveillance be prohibited or that any platform be sanctioned, but to assess whether the existing consent framework sustains a coherent doctrinal structure in this context, and to construct, from materials already present in Indian law, the doctrine that a coherent answer requires.

3.2 Research Strategy: Single-Site Doctrinal Case Study

The strategy combined doctrinal analysis with a single-site case study, in which MyGate, situated within the residential housing market of Mumbai, served as the concrete instance through which the doctrinal question was examined. The case study was not selected to generate generalisable empirical claims about the platform's conduct, but because doctrinal coherence is best tested against a specific and representative fact pattern, and because the conditions under which the consent question becomes acute, namely market saturation, acute housing unaffordability, and dense vertical development, obtain in Mumbai with unusual clarity.

MyGate was chosen on two grounds. It is the dominant platform in the residential management space, and its functional architecture, integrating entry management, visitor logging, movement records, third-party services, and financial transactions within a single application, makes it representative of the broader category rather than an outlier. Its findings were treated as illustrative of the structural problem common to that category, including the competing platforms NoBrokerHood, ApnaComplex, and ADDA, and not as claims peculiar to one firm.

3.3 Data Sourcing and Inclusion Criteria

The research was desk-based, drawing on both primary and secondary sources. The primary materials comprised the relevant provisions of the DPDPA and the Indian Contract Act, the report of the Committee of Experts chaired by Justice B. N. Srikrishna, and the several opinions in *K. S. Puttaswamy v. Union of India*. The secondary materials comprised scholarship on Indian data protection, the theoretical literature on surveillance and extraction, the apparatus of contextual integrity and the analysis of rights, and investigative reporting on the conduct of residential platforms. The factual predicate concerning MyGate was drawn from this last category, principally the reporting of Kodali and Kissu and the platform's own published documentation, since no primary fieldwork was undertaken.

Inclusion was governed by doctrinal and theoretical relevance rather than descriptive breadth. Sources were included where they illuminated how consent is constructed, interpreted, or displaced, how residential data collection escapes the protection the law nominally affords, or why certain intrusions lie beyond the reach of individual waiver. Sources were set aside where their orientation was purely empirical, journalistic, or advocacy-driven without sustained engagement with the doctrinal or theoretical questions at issue, except where necessary to establish the factual context of platform conduct.

3.4 Method of Analysis

The analysis treated data protection law not as a set of discrete rules but as a structured argumentative system whose legitimacy depends on the consistent operation of its organising principle. The four statutory criteria of valid consent, that it be free, specific, informed, and capable of withdrawal, were taken as the indicators against which the residential enrolment was tested, each examined in turn. For each, the analysis established the doctrinal content of the criterion from the statute and its legislative history in the Srikrishna report, applied that content to the conditions of residential enrolment as exemplified by MyGate, and drew on the theoretical literature to explain why the failure observed was structural rather than incidental. The contextual-integrity framework was applied to the specific and informed criteria, the natural-rights and Hohfeldian analysis to the question of whether the platform held the power to extract a waiver at all, and the medical-consent doctrine of *Samira Kohli* was adapted, as a doctrinal transplant, to the question of revocability.

The method carries limitations that bound its claims. The study is doctrinal and not empirical, establishing the structural unattainability of valid consent as a matter of legal coherence without measuring how residents in fact experience enrolment or how platforms in fact deploy the data they collect. Its factual predicate rests on investigative reporting and platform documentation rather than independent verification, its argument is anchored in a single platform and city whose extension to the wider category is reasoned rather than demonstrated, and it and it addresses the framework in its completed form, the Act together with the Rules notified under it, in the period before their substantive commencement. These limitations bound the paper's claims without weakening its central contention, which concerns the coherence of the consent framework rather than the empirical incidence of its failure.

PART IV — DISCUSSION

THE STRUCTURAL FAILURE OF RESIDENTIAL CONSENT

4.1 The Architecture of Residential Surveillance

The literature closed on a question rather than a finding, whether the consent obtained at the residential threshold can satisfy the criteria the statute lays down, and that question cannot be reached until the object of the consent is in view. The resident agrees to something the platform presents as narrow, a convenience for admitting visitors and settling bills, and the analysis must

set that presented object beside the thing actually built. The distance between the two is where the structural failure first becomes legible.

What is built is a continuous record. The platform timestamps the resident's entries and exits, files each visitor by name, photograph, number, and stated purpose, logs the domestic workers attached to the household, and registers vehicle movement as it happens. Each function is defensible on its own as a security measure, and that individual defensibility is what conceals the aggregate, because the functions accumulate into precisely the individual the review identified, the resident resolved into discrete coordinates and reassembled, by the platform rather than by her, into a profile she has never seen. The concept does its work here without further elaboration, because what Deleuze named in the abstract the entry log builds in the concrete.³³

The question the review left Deleuze unable to answer, why anyone would construct so elaborate a decomposition of people who have done nothing, the architecture answers in its data flows. The record moves beyond the gate along channels the platform itself discloses, to the society's administrators, to neighbours through the social layer whose leakage residents register as the spam that follows enrolment,³⁴ and into a commercial layer the platform runs over its own base. That commercial layer is not incidental to the security function but wired directly into it, most plainly in the advertising the platform serves at the moment of entry approval, where the card a resident taps to admit or deny a visitor is itself an advertising surface and each visitor entry generates a further placement.³⁵ The same fusion drives the platform's express-entry integration, through which delivery and marketplace applications connect to MyGate by interface so that a resident's order on a partner application triggers a pre-approval request at her own gate, offered to partners as an operational efficiency and sold to residents, in its automated form, as a premium tier.³⁶ This is Zuboff's surplus taking its specific residential form, the rendition of a household's rhythm into a prediction the platform is built to monetise,³⁷ and it supplies the motive the decomposition otherwise lacks. The machine is elaborate because

³³ Deleuze (n 8) 5.

³⁴ Sagrika Kisku, 'Gurugram Gate Apps Know Everything. Privacy vs Convenience Is Dividing Condos' *ThePrint* (21 April 2025) <https://theprint.in/ground-reports/gurugram-gate-apps-know-everything-privacy-vs-convenience-is-dividing-condos/2595465/> accessed 8 July 2026.

³⁵ Vaishali Tripathi, 'MyGate Advertising – Types, Ad Targeting & Facts' *The Media Ant* (8 June 2023) <https://www.themediant.com/blog/mygate-advertising-types-and-audience-targeting/> accessed 8 July 2026.

³⁶ Kamesh, 'The Nth Order Effect: MyGate's Early Approvals Impact on Last-Mile Delivery ETA' *The Product Town* (8 January 2025) <https://theproducttown.substack.com/p/the-nth-order-effect-mygates-early> accessed 8 July 2026.

³⁷ Zuboff (n 12) 8.

the surplus is worked, and a society installs it not to watch its residents but to convert them into supply.

The platform completes the manoeuvre by disowning the very role its conduct establishes. It describes itself as a processor acting for the society and casts the society as the fiduciary, and its founder disclaims custody of the record in terms, the data belongs to the associations and not to the platform.³⁸ The statute fixes the fiduciary as whoever determines the purpose and the means of processing, and a platform that designs the profile, sets the retention, and runs the commercial layer over the record determines both,³⁹ so the disclaimer describes a role the architecture contradicts. Each branch of the disclaimer fails the resident in the same way. If the platform is the fiduciary it denies being, the consent it frames is a fiduciary's and must satisfy every criterion the statute sets and does not, and if it is the processor it claims, the society is the fiduciary that owed the resident a valid consent and obtained none, having resolved the matter in a committee she did not sit on, a position taken up among the objections below.

The platform's terms then perform the move the review marked as contestable, asserting proprietary right over the processed record as the platform's own intellectual property. The claim cannot survive Zuboff's distinction between the behaviour that furnished the raw material and the processing that merely refined it, since the resident's movement was the input and the platform's analytics only its appropriation, which means the proprietary assertion describes a taking in the grammar of ownership. The resident is positioned as the customer of a security service when she is, in the architecture's own logic, its raw-material supplier, the source of the surplus while the paying customers stand downstream. A consent given on the understanding that she is the buyer is addressed to a relationship the architecture inverts, and a consent addressed to a relationship that does not exist secures nothing the platform actually does.

The inversion is widened by the breadth the single login is made to carry, the vehicle registration, the payment history, the staff directory, the neighbours' numbers, and the timestamped record of every coming and going at one door. A platform that began as the digital successor to the security guard's paper register now holds a fuller account of a household's day than the household keeps of itself, installed in most societies because a committee resolved once that everyone would use it. Privacy here is not eroded but, in Zuboff's exact sense,

³⁸ Abhishek Kumar (co-founder and CEO, MyGate), quoted in KISSU (n 34): 'we are not the custodians of the data. The data belongs to the RWAs.'

³⁹ Digital Personal Data Protection Act 2023, s 2(i) (definition of Data Fiduciary).

redistributed,⁴⁰ the decision over what the home discloses lifted from the resident and relocated to the platform and the committee that bound her to it.

That relocation is the doctrinal heart of the matter, because the statute makes consent the act by which a person retains the decision the architecture has already moved. A single agreement, given once at the threshold to an object understood as narrow, is treated as authority for an extraction scaled not to a gate but to a life, and the defect is not informational, curable by fuller notice, but structural, residing in a bargain that converts one act of agreement into a warrant for everything the architecture performs. This mismatch between the small thing consented to and the large thing done is the pattern's first and plainest appearance, and each statutory criterion that follows is a further doctrinal name for the same structural fact. The criterion the statute names first, and the one this architecture most immediately offends, is whether a consent so obtained can be called free.

4.2 The First Failure: Consent That Is Not Free

The architecture established that the resident's decision over what her home discloses has already been relocated to the platform, and the statute's first criterion is the demand that whatever consent she gives be free. Section 6 of the DPDPA conditions all lawful processing on a consent that is, in the provision's own terms, free, specific, informed, unconditional, and unambiguous,⁴¹ and the word free is not left to float, because the Srikrishna Committee that authored the architecture of the provision fixed its meaning in a single operative rule. Consent, the Committee held, cannot be made a condition for the provision of a service unless the processing is necessary for that service.⁴² The residential arrangement closely resembles the kind of bundling the Committee appears to have sought to prohibit. Whether it falls within that prohibition depends on how "necessary processing" is understood.

Necessity is the hinge the architecture severs. Admitting a visitor requires verifying a visitor, and no part of that function requires that the verification be retained for months, aggregated into a behavioural profile, or fed into the commercial layer the platform runs over its base, so that the processing the enrolment exacts runs far beyond the processing the service needs. The Committee treated that surplus exaction as the destruction of freedom and not a defect at its

⁴⁰ Zuboff (n 12) 10, 48.

⁴¹ Digital Personal Data Protection Act 2023, s 6(1).

⁴² Srikrishna Committee (n 21) 34.

margins, because consent demanded for more than the service requires is not consent the person was ever free to refuse in part. The resident is offered not access conditioned on necessary processing but access conditioned on submission, and submission exacted under the colour of necessity is, on the Committee's own rule, the mark of a consent that is difficult to reconcile with Section 6's requirement of free consent.

What the Committee reached through legislative design, the contract scholarship the review assembled reaches through the doctrine of assent, and the two arrive at the same place from opposite ends. Radin's account of boilerplate names the residential enrolment for what it is in private law, a "private eminent domain" in which the resident is conscripted into a legal universe of the platform's devising as the price of a transaction she cannot decline,⁴³ while Kim's analysis of the adhesive form locates the defect beneath the click,⁴⁴ in the absence of any genuine assent where the only alternatives are acceptance or exclusion. Where Srikrishna says the bundling destroys freedom, Radin and Kim say the form was never assent to begin with, and the convergence is the argument, because a consent that fails the statute's freedom criterion and the older contractual test of assent at once is not failing by the standard of one rule but by the shared standard of consent itself.

The doctrine those scholars describe is not foreign to Indian contract law, which states the same requirement in its own terms. The Indian Contract Act makes free consent the condition of a binding agreement, and defines it negatively, as consent not caused by coercion, undue influence, fraud, misrepresentation, or mistake.⁴⁵ The residential enrolment is coerced in a sense the Act's enumerated categories do not quite reach, and the gap is instructive rather than fatal. It is not the coercion of Section 15, which requires an unlawful threat, because the platform threatens nothing forbidden by law, and it is not cleanly the undue influence of Section 16, which requires a relationship in which one party dominates the will of another, because the pressure on the resident is exerted by the structure of the housing market rather than by a dominating counterparty.⁴⁶ What the residential case presents is a coercion that is structural and lawful at once, market coercion that vitiates the freedom of consent while fitting none of the vitiating categories the Act names, and the very fact that established contract doctrine has

⁴³ Radin (n 29) 15.

⁴⁴ Kim (n 30).

⁴⁵ Indian Contract Act 1872, ss 10 and 14.

⁴⁶ Indian Contract Act 1872, ss 15 (coercion) and 16 (undue influence).

no ready home for it is what marks the residential bargain as a problem the existing law states but does not resolve.

The comparative regime the DPDPA was modelled upon completes the convergence from a third direction. The European framework treats consent bundled with access to a service the processing does not require as consent that cannot be regarded as freely given,⁴⁷ and Recital 43 states without qualification that consent is presumptively not free where there is a clear imbalance between the parties.⁴⁸ The imbalance between a resident and a platform installed by her housing society, integrated with her tenancy and operated beyond her inspection, is the paradigm the Recital describes, and the rule it yields is identical to the rule Srikrishna drafted and the principle Radin and Kim defend. When legislative design, contract doctrine, and the comparative standard the statute borrowed all converge on the same conclusion, the proposition that residential enrolment cannot produce free consent ceases to be one reading among several and becomes the settled structure of the consent the law requires.

The platform's reply is that no submission occurs because the resident remains free to decline, and the reply collapses on the structure of the market in which the choice is set. Zuboff's landlord, conditioning tenancy on access to a prospective tenant's social media, is not an analogy fetched from elsewhere but the residential case in its original statement, and her observation that it is those "with the least resources and the fewest options" who are caught in the bargain identifies precisely who,⁴⁹ in Mumbai, confronts the choice. A right to refuse exercisable only by surrendering housing, in a market where the reachable alternatives run the same platform, is a right to refuse in name alone, and a freedom that costs the home from which it is exercised is not the freedom Section 6 demands.

The political economy the review assembled explains why that choice is structurally absent rather than merely difficult. The enclosure Varoufakis describes is not a figure of speech in a saturated residential market but the literal condition of a tenant for whom every accessible society runs the same architecture,⁵⁰ so that the exit the platform's defence presupposes does not exist to be taken. Consent presupposes an outside, a position from which refusal leaves the person no worse than she was, and saturation abolishes the outside. Where there is no outside

⁴⁷ GDPR (n 31), art 7(4).

⁴⁸ *ibid*, recital 43.

⁴⁹ Zuboff (n 12) 174.

⁵⁰ Varoufakis (n 11) 3.

there is no refusal, and where there is no refusal the agreement that remains is ratification of a *fait accompli*, not consent to a proposal.

The failure widens once the resident is set beside the others the same enrolment binds. The domestic worker logged against her employer's account, the visitor filed without being asked, the delivery rider tracked through the society, none has been offered even the formal choice the resident declined, and the data of each is taken on the authority of a consent given by someone else. This is the condition in which one person's agreement purports to authorise the processing of another who has neither visibility into the arrangement nor any power to withdraw from it, and the residential gate is where that failure is most complete. A consent that binds those who never gave it is not a defective consent at all but the absence of consent operating under consent's name.⁵¹

The freedom criterion fails, then, along two distinct lines that share a single root. The resident's own agreement is unfree because the saturated market leaves her no outside from which to refuse, and the surveillance reaches third parties her agreement was never competent to bind, so that the defect is not that consent was given badly but that the conditions under which valid consent could be given were absent before the enrolment was ever presented. Three independent bodies of law, statutory, contractual, and comparative, converge to establish the first proposition, and the structural-failure principle establishes the second, which leaves the platform defending a freedom that exists in neither the resident's position nor those of the people her consent purports to speak for. The statute next asks whether the consent, supposing it free, was at least specific to a defined purpose, and the architecture's answer is that a single enrolment dissolves the very boundaries on which specificity depends.

4.3 The Second Failure: Consent That Is Neither Specific Nor Informed

Suppose the freedom objection answered and the resident's agreement treated, for argument, as freely given. Section 6 demands more, that the consent be specific to a stated purpose and informed as to what it authorises,⁵² and these two requirements fail together in the residential case because they fail for one reason. The enrolment dissolves the boundary between the

⁵¹ See Srivastava and Chaudhari (n 24) 5–7.

⁵² Digital Personal Data Protection Act 2023, s 6(1).

purpose the resident understands and the purposes the architecture serves, and a consent that cannot locate its own object can be neither specific to it nor informed about it.

Specificity is a requirement about boundaries, that consent given for one purpose does not travel to another, and the contextual-integrity principle the review established supplies the standard by which the boundary is drawn.⁵³ Information surrendered at the gate is surrendered within a context whose norms are those of residential security, the verification of who enters, and the legitimacy of any onward flow is governed by those norms and not by the bare fact that the resident clicked. When the entry record leaves the security context and arrives in the context of commerce, in the platform's advertising business, in its e-commerce and delivery integrations, in analytics that predict the resident rather than admit her visitor, the flow crosses a boundary the originating context never authorised. The violation is not that the data was collected but that it migrated, and a consent given to the gate cannot reach the profiler because the two stand in contexts the resident's agreement was never addressed across.

Chandrachud's plurality opinion reaches the same boundary from the constitutional side,⁵⁴ and the meeting of the two sources hardens the doctrinal claim that theory alone would leave contestable. Where Nissenbaum derives the limit from the norms that constitute a context, Chandrachud derives it from the principle that information yielded in one relationship cannot be redirected to another without consent specific to the redirection, and an Indian court reasoning from privacy and an American theorist reasoning from information flow converge on the proposition the statute's specificity limb already contains. The convergence matters because it places the specificity requirement beyond the platform's reach. Consent to verification at the gate is not consent to profiling in the prediction market, and a single enrolment that treats the first as authority for the second has not satisfied specificity but abolished it.

The informational limb fails on the same structure, because a resident cannot be informed about a flow whose destination is concealed by design. The surveillance-capitalism account the review assembled established that the opacity is not a failure of disclosure to be cured by a fuller notice but a built feature of the model, since the value of the surplus depends on uses determined after collection and hidden from the person collected from. A notice that disclosed

⁵³ Nissenbaum (n 18) 119–20, 125.

⁵⁴ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (306)–(310) (Chandrachud J) (purpose limitation and informational self-determination).

the gate function in full would still not inform the resident of the profiling, because at the moment of enrolment the profiling has no fixed purpose to disclose, only an open-ended intention to extract uses the platform has not yet decided upon. Consent cannot be informed as to purposes that do not yet exist to be stated, and a framework that demands informed consent for processing whose purposes are deliberately deferred demands what the architecture is built to withhold.

The deeper failure is one of aggregation, and it defeats the platform's most plausible reply. The platform will say that each individual record is innocuous, that a single timestamp recording a resident home at seven in the evening discloses nothing, and the point is correct and beside the point at once. The contextual-integrity literature locates the violation not in the individual record but in the aggregate, because entries and exits and visitor identities and absences, each contextually appropriate where it was generated, combine across time into a behavioural profile that exists in a different context entirely, the prediction market the individual data points were never released into. Each collection was contextually appropriate and the aggregate is a contextual violation, which means consent obtained collection by collection cannot validate a profile no single collection disclosed.

The platform's last move on this terrain is to claim that the context itself has changed, that residents now expect platform surveillance as the ordinary condition of gated living and that ubiquity has remade the baseline of reasonable expectation. The contextual-integrity principle refuses the move on principle and the refusal is decisive here. A practice cannot validate itself by the fact of its own spread, the prevalence of a departure from a norm does not convert the departure into the norm, and legitimate change in the norms of residential information requires deliberation rather than the accomplished fact of deployment. The burden lies on the departing practice to show that its departure serves a value weighty enough to justify the privacy it costs, and convenience and efficiency are not such values but the preferences the framework already distinguishes from them. That MyGate is now everywhere is not the answer to the objection that MyGate violates the residential norm, it is the restatement of the objection at scale.

Specificity and information therefore fail as one, because the architecture is built to dissolve exactly the boundaries the two requirements depend upon. The resident cannot consent specifically to a flow whose destination is concealed, cannot be informed of purposes deferred until after collection, and cannot, by agreeing collection by collection, authorise an aggregate that no collection revealed, and the ubiquity offered to cure these defects only generalises them.

What remains of consent once its object cannot be located is a signature on a boundary the architecture has already erased, and the statute's third demand, that the consent remain revocable, meets an architecture designed to ensure that what has been taken cannot be returned.

4.4 The Third Failure: Consent That Cannot Be Withdrawn

The architecture of specificity closed on a system built to ensure that what it takes cannot be returned, and the statute's third demand meets that system directly. Section 6 requires that consent be as easy to withdraw as to give,⁵⁵ and the requirement is not ornamental, because a consent that cannot be retracted is not a continuing authorisation but a single irreversible surrender. The residential enrolment offers withdrawal in form and forecloses it in substance, and the doctrine that exposes the foreclosure is one Indian law has already built in a setting whose structure the residential case reproduces.

That setting is medical consent, and *Samira Kohli* is its governing statement.⁵⁶ The Court held there that consent is specific to the procedure disclosed, that consent to a diagnostic procedure does not authorise a therapeutic one, and that a materially different or additional intervention requires fresh consent unless a genuine emergency makes obtaining it impossible. The holding is not itself a doctrine of revocation, but its structure carries one, because a consent that is exhausted by the specific procedure it authorised and cannot stretch to cover what was not disclosed is a consent that treats authorisation as ongoing and bounded rather than given once and for all. The holding is usually read as a rule about surgery, but its reasoning rests on three structural conditions, and those conditions, not the surgical setting, are what give the rule its force. The transplant to residential surveillance is legitimate precisely because all three conditions hold there as fully as they hold in the operating theatre.

The first condition is an ongoing relationship rather than a discrete transaction. The surgeon's authority is not exhausted at the moment of incision but persists through a procedure that unfolds over time, which is why consent must persist and remain revocable across it, and the residential platform's processing is continuous in exactly this sense, not a single act of collection at enrolment but an open-ended operation that runs for the length of the tenancy. A consent adequate to a one-time transaction is inadequate to a relationship that continues,

⁵⁵ Digital Personal Data Protection Act 2023, s 6(4).

⁵⁶ *Samira Kohli v Dr Prabha Manchanda* (2008) 2 SCC 1 [42]–[44], [55]–[60].

because the person cannot foresee at the outset what the relationship will later do, and the platform's processing, like the surgeon's procedure, is a relationship and not a transaction. Consent given once at its threshold cannot authorise everything it will later perform.

The second condition is opacity, the impossibility of evaluating from outside what the expert system does within. The patient cannot assess the clinical judgment that the surgeon exercises under anaesthesia, which is why the law supplements her initial consent with a continuing right to refuse rather than treating the first signature as conclusive, and the resident stands in the same darkness before the platform's processing. The surveillance-capitalism account established that the opacity is structural and not incidental, that the resident cannot know what the aggregate of her records will be made to reveal because the uses are determined after collection and concealed by design. Where the person cannot evaluate what she has authorised, the initial consent cannot be conclusive, and the law's answer in the medical case, a continuing power of withdrawal, is the answer the residential case requires for the identical reason.

The third condition is power asymmetry, the structural inequality between an individual and an expert institution that defeats the assumption of arm's-length agreement. The patient does not meet the surgeon as an equal and the law accounts for the inequality by refusing to treat her initial consent as a complete waiver, and the resident meets the platform, the housing society, and the landlord across an asymmetry of exactly the kind, magnified by the saturated market the freedom analysis established. The three conditions that justify a continuing and revocable consent in the residential case, drawn from the structure *Samira Kohli* established, an ongoing relationship, an opaque expert process, and a structural inequality of power, are not analogues of the residential situation but a description of it, and a doctrine built on those conditions governs wherever they recur.

The Indian data-protection literature reached the same destination from the side of the platform rather than the patient. Srivastava and Chaudhari, examining relational data, ground the defect in privity of contract, showing that where one person's consent purports to authorise processing of data generated by and about another, that second person is bound by a contract she was never party to and cannot withdraw an authorisation she never gave.⁵⁷ The residential gate reproduces this defect and extends it, because the resident cannot withdraw on her own behalf where the market forecloses exit, and she cannot withdraw on behalf of the visitors and workers her

⁵⁷ See Srivastava and Chaudhari (n 24) 5–7.

enrolment binds because their data was never hers to retract. A withdrawal right that the rights-holder cannot exercise and that does not reach the persons most exposed is not a right that is difficult to exercise, it is a right that does not function as one.

The platform's answer is the consent-manager dashboard, the interface through which the resident may toggle her permissions and so, the platform says, withdraw at will, and the answer is no longer merely the platform's, since the Rules notified under the Act have given the mechanism statutory form.⁵⁸ The answer mistakes the location of the defect. A dashboard governs the permissions the architecture chooses to expose, not the processing it has structured to run regardless, and where withdrawal of the commercial processing is made to entail loss of the security function the tenancy depends upon, the toggle is not a power of withdrawal but a restatement of the original coercion in a smaller frame. The problem the withdrawal right confronts is upstream of any interface, in a bargain that conditioned the home on the processing, and an interface downstream of that bargain cannot return what the bargain was structured to keep. Revocability offered on the platform's terms is revocability the platform has already defeated, and an interface certified by the state is still an interface.

The revocability criterion therefore fails for the same structural reason as the two before it. The processing is a continuing, opaque, and asymmetric relationship that the medical doctrine identifies as demanding a real power of withdrawal, the relational character of the data places that power beyond the resident's reach for those her consent purports to bind, and the interface offered as a remedy operates downstream of a coercion it cannot touch. Three criteria have now failed, freedom, specificity with information, and revocability, and they have failed not independently but for a single recurring reason that each expresses in its own register. What that reason is, and why it means the consent framework cannot be repaired by improving any one criterion, is the question the analysis must now confront directly.

4.5 Why the Consent Framework Cannot Be Repaired

Three criteria have failed, and the temptation is to read the failures as a list of repairable defects, to suppose that a freer market would cure the first, a narrower notice the second, an easier withdrawal the third. The supposition mistakes symptoms for the disease. The three failures

⁵⁸ Digital Personal Data Protection Rules 2025, notified 13 November 2025, published in the Gazette of India, 14 November 2025 (made under s 40 of the Digital Personal Data Protection Act 2023), r 4 and First Schedule. The Consent Manager framework and its bearing on the residential case are addressed in section 4.5 below.

share a single structural cause, and naming it is the work of this section, because a framework whose criteria fail for one reason cannot be repaired by improving the criteria one at a time.

The common element is visible once the three failures are set beside one another. Freedom failed because the resident could not refuse without losing the home, specificity and information failed because the home's data could not be sealed within the context it was generated in, and revocability failed because the processing could not be exited without losing the home again. In each the home is the hinge, the necessity that makes refusal impossible, the context whose norms are breached, the dependency that forecloses withdrawal. The consent fails at every criterion because the surveillance is built into the infrastructure of a necessity the resident cannot leave, and a consent extracted as a condition of infrastructure one cannot exit is not a species of consent the criteria can rehabilitate. It is a category the framework was not built to govern, which this paper names infrastructural consent.

Infrastructural consent is defined by three features that the preceding analysis established without yet naming, and each is what disables one criterion. The first is non-separability, that the surveillance cannot be declined without forfeiting the underlying necessity, which is what defeated freedom. The second is structural opacity, that the processing cannot be evaluated by the person subjected to it because its uses are deferred and concealed, which is what defeated specificity and information. The third is temporal continuity, that the relationship runs for the length of the tenancy rather than closing at a moment of agreement, which is what defeated revocability. A consent given under all three conditions at once is not weak consent to be strengthened but consent addressed to the wrong object, because notice-and-consent assumes a discrete transaction between separable parties, and infrastructural consent is the absorption of a person into a system from which separation is the very thing foreclosed.

This is the point at which the natural-rights apparatus the review assembled does its decisive work, because it explains why the defect is not one of degree. Finnis's reconstruction of Hohfeld supplies the category the residential right belongs to, the immunity,⁵⁹ the position in which one party simply lacks the power to alter another's legal standing, and a privacy so construed is not a liberty the resident trades but a position the platform has no power to change. The consequence reaches deeper than any criterion. The defect at bottom is not that the resident's consent was unfree, unspecific, or unwithdrawable, though it was each, but that the platform

⁵⁹ Finnis (n 25) 199–205.

never held the power to extract a valid waiver at all, because the right was structured as an immunity against precisely that exercise of power. A defective consent can be cured by curing the defect. A consent the other party had no power to take cannot be cured at all.

The characterisation invites three objections, and each returns the analysis to the same ground. The first asks why the right is cast as an immunity rather than a claim-right, since a claim-right against intrusion would seem to do the same work. It would not, because a claim-right correlates to a duty the platform owes and could in principle discharge or breach, and the argument here is not that the platform owes a duty it has failed to perform but that it lacks the power to alter the resident's position at all, which is the immunity and not the claim.⁶⁰

The second asks whether immunity is merely inalienability wearing a borrowed vocabulary. It is not, because inalienability describes the consequence, that the right cannot be surrendered, while the immunity describes the cause, the absence in the platform of any power to receive the surrender, and it is the cause and not the consequence that explains why no improvement to the consent could succeed.

The third asks why the argument reaches for Hohfeld rather than resting on dignity, and the answer is that dignity is the register of the constitutional claim this paper has deferred, while the immunity is the structure the private-law claim requires, a claim about the distribution of legal powers between two private parties rather than about the moral weight of the interest at stake. The immunity analysis is therefore not an ornament on the consent argument but the thing that completes it, the account of why a consent repaired at every criterion would still fail, because the party seeking it never held the power the repair presupposes.

Nariman's formulation in *Puttaswamy* supplies the same ceiling from the constitutional side, and it is invoked here for the strength it lends the consent claim and not as an independent ground. Privacy, he held, is recognised by the Constitution and not granted by it,⁶¹ which is the constitutional statement of the structural point that one cannot surrender through contract what one did not receive through contract in the first place. A right that positive law recognises rather than confers cannot be exhausted by the instruments of positive law, and a contractual term purporting to waive it operates on something the contract did not create and so cannot, by its own authority, destroy. The platform's enrolment is positive law in miniature, a private

⁶⁰ Finnis (n 25).

⁶¹ *Puttaswamy* (n 26) 598, 601 (Nariman J).

instrument asserting a power over a right that precedes it, and a private instrument cannot extinguish what the Constitution itself only acknowledges.

That the right resists waiver is not a peculiarity of privacy but a feature of the class of right it belongs to. Finnis distinguishes rights one exercises from rights that protect against a specified wrong,⁶² the latter carrying a conclusory force that mere preference-rights lack, and the right not to have one's home rendered into a continuous behavioural record as the price of occupancy belongs to the second class. Hart, defending the choice theory that makes *waivability* the core of a right, conceded that the theory fails for rights grounded in basic human need rather than individual choice,⁶³ and the concession is fatal to the notice-and-consent model in this setting, because that model treats every right as a preference its holder may trade. A right that exists to protect a basic condition of personhood is not held as a chip to be wagered at a gate, and a framework that can only conceive of consent as the exercise of such a chip cannot register the kind of right the home engages.

The surveillance-capitalism account names the same defect in the register of power rather than right. The decision over what the home discloses was, in Zuboff's exact sense, not eroded but redistributed,⁶⁴ lifted from the resident and concentrated in the platform, and consent is the instrument that launders the redistribution into the appearance of a transfer the resident authorised. Kaul's observation in *Puttaswamy*, that truthful information whose disclosure breaches privacy may still require protection, completes the point,⁶⁵ because it severs the legitimacy of a flow from the accuracy or the formal authorisation of the data within it. That the entry logs are truthful and the enrolment formally signed does not redeem the extraction, since the wrong is the redistribution of the decision and not the falsity of the record, and consent that ratifies a redistribution it had no power to authorise has legitimated nothing.

The objection that the framework has not yet been given its chance is the most serious that can be made against this analysis, and the Rules notified under the Act in November 2025 are where it must be met.⁶⁶ Those Rules answer the bundling and withdrawal defects with an architecture of their own, the Consent Manager, an interoperable platform through which a principal may

⁶² Finnis (n 25) 209–10.

⁶³ *ibid* 206, quoting HLA Hart, 'Bentham on Legal Rights' in AWB Simpson (ed), *Oxford Essays in Jurisprudence: Second Series* (Clarendon Press 1973) 171, 200.

⁶⁴ Zuboff (n 12) 10, 48.

⁶⁵ *Justice KS Puttaswamy (Retd) v Union of India* (n 20) 619–20 (Kaul J).

⁶⁶ DPDP Rules 2025 (n 58).

give, review, manage and withdraw consent, registered with the Board, independently certified, capitalised at not less than two crore rupees, barred from acting as fiduciary or processor for the principals it serves, and bound to retain the record of every consent for seven years.⁶⁷ The design is careful and its intent is unmistakable. If consent has failed because it is bundled, opaque, and practically irrevocable, the state's answer is to build the resident an instrument through which consent can be unbundled, inspected, and revoked at will.

The instrument does not reach the residential case, and the reason it does not is the reason the whole framework does not. A Consent Manager is an interface, and the defect in residential enrolment is not located at any interface. The resident who withdraws her consent through a certified and interoperable platform withdraws it from a fiduciary whose service is the condition of her tenancy, so that the withdrawal costs her the security function the society requires her to use and, in the end, the home in which she uses it.

The conflict-of-interest bar sharpens the point rather than softening it, because a platform that cannot serve as its own Consent Manager will simply have the resident's revocation routed through a third party while the architecture, the society's resolution, and the tenancy remain precisely as they were. What the Rules perfect is the mechanism of consent. What they leave untouched is the condition under which it is given, and a mechanism perfected inside a bargain that cannot be refused is a better instrument for recording the same coerced agreement.

The withdrawal the Rules guarantee is, moreover, a withdrawal the resident cannot make on behalf of anyone but herself. The domestic worker logged against her account, the visitor filed at the gate, the courier cleared through the entry system, none of these acquires a Consent Manager by the resident's use of one, and none can revoke through her interface a consent she gave and they never did. The Rules assume a principal who holds her own data and may retrieve it. The residential gate produces principals who hold each other's, and it is the second condition, not the first, that the architecture creates.

The timing is what gives the argument its urgency rather than blunting it. Rule 4 commences in November 2026 and the substantive obligations, the notice standards, the retention and erasure triggers, and the rights of data principals, commence on 14 May 2027, so that the regime this paper examines has been enacted, elaborated, and scheduled, but not yet made to

⁶⁷ *ibid* r 4 and First Schedule, Parts A and B.

confront the class of consent it will be least able to police.⁶⁸ The framework will arrive at the residential threshold with an apparatus built for a transaction between separable parties and will find a relationship in which separation is the thing foreclosed. That confrontation has not yet happened, and the doctrine this paper proposes is offered before it does.

The framework cannot be repaired, then, because every repair operates on a criterion while the defect lies beneath all of them, in the infrastructural character of the consent and the immunity-structure of the right it cannot reach. A freer market, a fuller notice, an easier toggle would each address a symptom and leave the disease, because none of them touches the fact that the surveillance is built into a necessity the resident cannot exit and addressed to a right the platform has no power to take. What the residential case requires is therefore not a better consent but a doctrine that recognises when consent is the wrong instrument altogether, and the objections that such a doctrine must answer before it can be stated are the subject of the section that follows.

4.6 Objections

A doctrine that finds consent incapable of authorising residential surveillance invites a series of objections, and the doctrine is worth stating only if it survives them. Five are serious enough to require an answer, and each, pressed to its end, turns out to confirm the structure it was raised to dispute.

The first objection is that the platform delivers genuine security, that residents want the gate managed and the visitors verified, and that the consent therefore reflects real demand rather than manufactured submission. The objection conflates two functions the analysis has kept apart. Wanting a visitor verified is not wanting that verification retained for months, profiled, and worked into the platform's commercial layer, and the security function the resident values is separable from the commercial extraction the enrolment attaches to it, technically separable because verification needs no permanent behavioural record, and doctrinally separable because the no-bundling rule requires exactly that the necessary be severed from the unnecessary.

The proportionality the constitutional jurisprudence applies asks whether a less invasive

⁶⁸ *ibid* r 1(2)–(4).

alternative would serve the security purpose in a real and substantial manner,⁶⁹ and a logbook, a one-time code, a visitor register plainly would. That a system delivers a benefit the resident wants does not license every extraction the system attaches to the benefit, and the genuineness of the security is not a defence of the surveillance but the bait that makes the surveillance saleable.

The second objection denies the premise of coercion altogether. The platform is not imposed upon the resident by a stranger but adopted by her own housing society, a body of which she is a member and in whose general meeting she may attend, speak, and vote. Collective decisions of that kind bind dissenting members as a matter of course, in the placement of a boom barrier, the hours of the gate, the engagement of guards, and the levying of maintenance, and no one supposes that a resident outvoted on the position of a barrier has been coerced into it. On this account the surveillance is not extraction imposed from outside but self-governance exercised from within, and the fiduciary is the society, which is to say the residents themselves. The objection is the strongest that can be made against the analysis, and it fails for three reasons that are worth taking separately.

It fails first because a collective decision cannot supply an individual statutory consent. The Act fixes consent in the Data Principal and requires that it be hers, free, specific, and informed, and it provides no mechanism by which a committee, a majority, or a body corporate may give that consent on her behalf. The statute knows how to authorise consent given by another and does so expressly for children and for persons with disabilities through their lawful guardians, and the absence of any equivalent provision for residents' associations is not a gap to be filled by analogy but the shape of the statute itself.⁷⁰ A resolution of the general body is not the consent of a data principal, and a platform that processes on the authority of such a resolution processes on an authority the Act does not recognise.

It fails second because the society's competence does not extend to the personal data of its members. The management of a co-operative housing society vests in its committee, which exercises only such powers as the Act, the rules, and the bye-laws confer, and the Act defines the object of a housing society as the provision to its members of dwellings and of common

⁶⁹ *Justice KS Puttaswamy (Aadhaar-5J) v Union of India* (2019) 1 SCC 1 (2753)–(2756) (Chandrachud J, dissenting) (necessity limb; less intrusive alternative).

⁷⁰ Digital Personal Data Protection Act 2023, ss 9(1) (children) and 9(2) (persons with disabilities), read with s 2(j) (definition of Data Principal).

amenities and services.⁷¹ The authority is real but it is bounded, and the boundary is the object. A resolution may determine where the gate stands, because the gate is a common amenity. It may not determine that the record of who passes through it belongs to a commercial platform, because that record is neither a dwelling nor an amenity, and a body whose powers are defined by its object cannot dispose of what lies outside it. The Hohfeldian point returns in its collective form, that the society lacks the power to waive what was never within its competence to waive, and the vote that is valid as to the barrier is void as to the data.

It fails third because the democracy on which the objection rests is in most cases absent and, where present, immaterial. The tenant is frequently not a member of the society at all, since membership in a cooperative housing society ordinarily attaches to ownership rather than occupation, so that the resident whose housing precarity the market analysis identified is bound by a decision taken in a body she cannot join, by persons whose interests are not hers. The owner who voted against the resolution, or who purchased after it, stands in the same position by a different route.

But the empirical point is the weaker one, and the objection does not improve if the democracy is made perfect, because a unanimous resolution of every member of the society would still fail for the two reasons already given. The society's authority over the building is not authority over the resident, and a body that may decide where the gate stands may not decide who owns the record of her passing through it.

The single ground with any purchase is Section 7(a), which permits processing of data a principal has voluntarily provided for a specified purpose and to whose use for that purpose she has not objected. The ground collapses into the analysis already made. It requires that the provision be voluntary, which the market coercion establishes it is not, and it confines the processing to the specified purpose for which the data was provided, which is the verification of entry and not the profiling that follows, so that Section 7(a) authorises the security function and stops precisely where the commercial extraction begins.

The provision that appears to rescue the platform re-imports the very limits the platform sought to escape, and the scholarship has already marked the danger, that Section 7(a) omits the

⁷¹ Maharashtra Co-operative Societies Act 1960, s 73(1) (management vested in the committee, exercising only such powers as are conferred by the Act, rules and bye-laws) and s 2(16) (defining a housing society by its object of providing members with dwellings and common amenities and services).

requirement of reasonable expectation its Singaporean model retains and so invites the repurposing of data beyond the use the principal envisaged.⁷² What the objection establishes, in the end, is not that the platform may proceed without valid consent but that the Act closes every route by which it might, and a statute that offers no lawful basis outside a consent that cannot be obtained has not licensed the processing, it has prohibited it.

The third objection is the gravest, that the DPDPA already governs this, that its consent provisions and its withdrawal right and its forthcoming consent-manager machinery cover the residential case, and that a new doctrine is therefore redundant. The objection fails on the same ground the revocability analysis exposed, that the Act's framework assumes a discrete transaction between a principal and a fiduciary and the residential relationship is neither discrete nor transactional.

The Act has no mechanism for the continuing, revocable consent that an infrastructural and ongoing relationship demands, no equivalent of the *Samira Kohli* rule that authorisation persists and remains withdrawable across a relationship that unfolds over time,⁷³ and it treats initial consent as conclusive precisely where the medical doctrine treats it as merely initial. The Act, in other words, supplies the four criteria and assumes a transaction in which to apply them, and the residential case is the relationship the transaction model does not see. A statute that governs the wrong unit of analysis does not cover the case, it misses it, and a doctrine that names what the statute misses extends the framework rather than duplicating it.

The fourth objection is that this is a privacy argument wearing the costume of consent, that the real complaint is surveillance of the home and consent is merely the instrument chosen to attack it. The objection inverts the actual order of the argument. The statute, not the paper, made consent the hinge on which lawful processing turns, and a paper that tests whether that hinge holds in the residential case is taking the statute's own chosen mechanism seriously rather than smuggling a privacy claim through it.

The argument does not assert that privacy outweighs consent. It demonstrates that consent, on the statute's own criteria, was never validly obtained, which means the processing is unlawful by the framework's own measure and not by an external privacy standard imported to defeat it.

⁷² Nandini Tandon and Mehul Sharma, 'When Consent Becomes a Paper Tiger: Section 7(a) of DPDPA, 2023 AND The Third-Party Doctrine' *NLS Forum* (1 September 2025) <https://forum.nls.ac.in/ijlt-blog-post/when-consent-becomes-a-paper-tiger-section-7a-of-dpdpa-2023-and-the-third-party-doctrine/> accessed 8 July 2026.

⁷³ Samira Kohli (n 56) [42]-[43].

To take a statute at its word and show its central mechanism failing on the statute's own terms is not to disguise a privacy claim, it is to decline the disguise the framework offers the platform.

The fifth objection is that courts should not author new consent doctrines, that the creation of legal categories belongs to Parliament and the judiciary should apply the DPDPA as written rather than supplement it. The objection has a short answer and a structural one. The short answer is that the Residential Consent Doctrine is not conjured from nothing but assembled from materials already in Indian law, the no-bundling rule the legislature itself endorsed, the continuing consent the Court itself articulated in *Samira Kohli*,⁷⁴ and the contractual limits on adhesive waiver the common law already enforces, so that recognising it is development of existing doctrine rather than the invention of new statute.

The structural answer is that *Samira Kohli* is itself the precedent, because the Court there did not wait for a medical-consent statute before holding that consent to surgery must be specific, informed, and continuing, but derived the requirement from existing principle and applied it to a setting the legislature had not addressed. A judiciary that built the continuing-consent doctrine for the operating theatre without legislative instruction is not legislating when it recognises the same doctrine at the residential gate, it is doing again, in a new setting, exactly what it has done before.

The five objections, taken together, leave the doctrine stronger than they found it, because each on inspection restates a feature of the structure rather than dislodging it. The security is genuine and that is why it sells, the exit exists and that is why it cannot be found, the statute applies and that is why it misses the relationship, the mechanism is consent and that is why the paper tests it, and the doctrine is judicial and that is why precedent already supplies it. What survives the objections is the finding the analysis reached, that consent cannot authorise residential surveillance because the surveillance is built into a necessity the resident cannot exit and addressed to a right the platform has no power to take, and what that finding requires by way of remedy is the doctrine the final part now states.

4.7 The Residential Consent Doctrine

If consent cannot authorise residential surveillance under the conditions the architecture imposes, the question is what conditions valid consent in this setting would have to satisfy, and

⁷⁴ *ibid* [62]-[67].

the answer is not a new statute but a doctrine implicit in the materials the analysis has already assembled. The Residential Consent Doctrine holds that consent to data processing obtained as a condition of residential occupancy is valid only where four requirements are met, each the direct correlate of one of the failures the discussion established, and none of them invented for the occasion. Where any is absent, the consent does not legitimate the processing, and the processing is unlawful by the framework's own measure.

The first requirement is that the security function be severed from the commercial one. Consent to residential surveillance is valid only for processing strictly necessary to the service the resident sought, the verification of entry, and a platform may not condition that service on consent to processing the service does not require, the retention, aggregation, profiling, and onward sale of the behavioural record. This is the Srikrishna Committee's no-bundling rule applied without dilution to the residential gate, and its effect is to make the security the resident wants available without the extraction she does not, so that a tenant may have her visitors verified without having her life rendered into supply. A platform that offers the gate only with the profiler attached has not obtained consent to either, because it has demanded consent to the bundle the rule forbids.

The second requirement is that consent remain genuinely revocable across the life of the tenancy, withdrawable as to the commercial processing without forfeiture of the security function or the home. The processing is a continuing relationship and not a closed transaction, and consent to it must persist in the form *Samira Kohli* recognised, specific to what was disclosed, continuing through the relationship, and revocable as it unfolds, so that the resident retains at every point the power to withdraw what she is not obliged to have surrendered permanently at the threshold. A withdrawal that costs the resident her security or her tenancy is not withdrawal but renewed coercion, which means revocability under the doctrine attaches to the commercial processing alone and may never be answered by degrading the necessity the resident cannot leave.

The third requirement is that residential data be sealed within the context of its collection. Information generated at the gate for the purpose of security may not flow to the contexts of behavioural profiling, third-party transfer, or financial assessment, because consent to collection within one context is not consent to migration across the boundary into another, and the aggregate profile that such migration builds is a wrong no individual collection disclosed or could authorise. The seal holds against the platform's claim that ubiquity has remade the

norm, because a practice does not license itself by spreading, and it holds regardless of the formal accuracy of the records within the flow, because the wrong is the migration and not the falsity of what migrates. Data lawfully collected at the gate becomes unlawfully held the moment it is put to a use the gate did not authorise.

The fourth requirement is the one that governs the other three, that the core of residential privacy is not waivable by the enrolment at all. The right not to have one's home rendered into a continuous behavioural record as the price of occupancy is structured as an immunity, a position the platform has no power to alter, and as a right recognised rather than granted it cannot be exhausted by a private instrument that did not create it. A consent purporting to waive that core does not waive it, because the power to extract the waiver was never the platform's to exercise, and the enrolment that asserts otherwise asserts a power positive law does not confer on a private party over a right that precedes it. Beneath the three operative requirements, then, lies a limit on what any of them can be made to surrender, and it is this non-waivable core that distinguishes the doctrine from a mere tightening of the consent the framework already requires.

Taken together the four requirements describe the consent the residential setting would need and the architecture is built to defeat, security severed from extraction, revocability that survives the tenancy, data sealed in its context, and a core that no enrolment can reach. The doctrine does not prohibit residential security platforms, it prohibits the conversion of residential security into residential surveillance under the colour of a consent that meets none of the conditions consent requires. What it asks of the law is not a new power but the consistent application of powers the law already holds, the no-bundling rule it endorsed, the continuing consent it articulated, the contextual limit its privacy jurisprudence implies, and the immunity its account of fundamental rights entails. The home that opened this inquiry, the threshold the law has always held most private, is the setting in which that consistency is now most urgently owed.

CONCLUSION

This paper began at the threshold of the home, the interior the law has always held most private, and found a checkpoint standing where the door used to be. The inquiry asked a single question, whether the consent obtained at that checkpoint, as the price of living behind it, can satisfy the criteria the Digital Personal Data Protection Act demands of it. The answer the analysis

returned is that it cannot, judged by the Act's own requirements and that the failure is not a defect at the margins of an otherwise sound arrangement but a failure at every criterion at once and for one reason.

The consent is not free, because the resident cannot refuse it without surrendering the home, in a market where the reachable alternatives run the same architecture and the outside that refusal presupposes has been abolished. It is neither specific nor informed, because the data surrendered at the gate cannot be sealed within the context of its collection, and the resident cannot consent specifically to flows whose destinations are deferred and concealed by design. It is not revocable, because the processing is a continuing relationship that the platform structures to ensure that what it takes cannot be returned. Three criteria, three failures, and beneath them a single structure.

That structure is what the paper has named infrastructural consent, the consent extracted as a condition of a necessity the person cannot exit, and it is what the notice-and-consent framework was never built to govern. The framework assumes a discrete transaction between separable parties, and the residential relationship is the absorption of a person into a system from which separation is the very thing foreclosed. This is why no repair confined to a single criterion can succeed, because a freer market, a fuller notice, or an easier withdrawal each addresses a symptom while the cause, the surveillance built into a necessity the resident cannot leave, remains untouched beneath all of them.

It is also why the deepest defect is not that the consent was given badly but that the power to take it was never the platform's to exercise. The right not to have one's home rendered into a continuous behavioural record as the price of occupancy is an immunity, a position the platform has no power to alter, and a right recognised rather than granted cannot be exhausted by a private instrument that did not create it. A consent that purports to waive what the enrolment had no power to take has legitimated nothing, and the redistribution of the decision over what the home discloses, from the resident to the platform, is not made lawful by the signature that records it.

What follows from this is not a demand for new legislation but the recognition of a doctrine the law's own materials already contain. Residential consent is valid only where the security function is severed from the commercial one, where withdrawal survives the tenancy without forfeiting the home, where data collected at the gate is sealed against migration to the profiler,

and where a core of residential privacy is held beyond the reach of any enrolment at all. These are not inventions but the consistent application of rules the law already holds, the no-bundling rule the legislature endorsed, the continuing consent the Court articulated, the contextual limit its privacy jurisprudence implies, and the immunity its account of fundamental rights entails.

The urgency lies in the timing, and the timing is now fixed. The substantive obligations of the framework commence on 14 May 2027, and the doctrine's justification grows stronger with every month that passes before them, because each society that adopts the architecture removes another exit and tightens the condition under which consent is extracted. A regime that arrives at the residential threshold after saturation is complete will find nothing left to protect, and the Consent Manager it brings with it will record, with certified interoperability and a seven-year audit trail, an agreement the resident was never in a position to refuse. The threshold of the home was the law's oldest boundary, the line beyond which observation required leave, and it is being redrawn, quietly and society by society, into a checkpoint that takes more than it returns and calls the taking consent. Whether that redrawing is permitted to stand is no longer a question the consent the platform obtains can answer, because that consent, on the law's own terms, was never the law's to give.

Bibliography

Primary Sources

Cases

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

Justice K S Puttaswamy (Retd) v Union of India (Aadhaar-5J) (2019) 1 SCC 1

Samira Kohli v Dr Prabha Manchanda (2008) 2 SCC 1

Legislation and Regulations

Digital Personal Data Protection Act 2023

Indian Contract Act 1872

Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1

Secondary Sources

Books

Finnis J, *Natural Law and Natural Rights* (2nd edn, Oxford University Press 2011)

Kim N S, *Wrap Contracts: Foundations and Ramifications* (Oxford University Press 2013)

Radin M J, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press 2013)

Varoufakis Y, *Technofeudalism: What Killed Capitalism* (Bodley Head 2023)

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019)

Contributions to Edited Books

Bailey R and Sane R, 'Regulating "Non-Personal Data": Developments in India' in Bart van der Sloot and Sascha van Schendel (eds), *The Boundaries of Data* (Amsterdam University Press 2024)

Hart H L A, 'Bentham on Legal Rights' in A W B Simpson (ed), *Oxford Essays in Jurisprudence: Second Series* (Clarendon Press 1973)

Journal Articles

Nissenbaum H, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 101

Reports

Committee of Experts under the Chairmanship of Justice B N Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)

Online Journal Articles and Blogs

Deleuze G, 'Postscript on the Societies of Control' (1992) 59 October 3

Tandon N and Sharma M, 'When Consent Becomes a Paper Tiger: Section 7(a) of DPDPA, 2023 and the Third-Party Doctrine' (*NLS Forum*, 1 September 2025) <https://forum.nls.ac.in/ijlt-blog-post/when-consent-becomes-a-paper-tiger-section-7a-of-dpdpa-2023-and-the-third-party-doctrine/> accessed 8 July 2026

Working Papers and Institutional Publications

Srivastava A and Chaudhari N, *Social Graph Portability* (Data Catalyst 2019)

Newspaper and Online News Articles

Kissu S, 'Gurugram Gate Apps Know Everything. Privacy vs Convenience Is Dividing Condos' *ThePrint* (21 April 2025) <https://theprint.in/ground-reports/gurugram-gate-apps-know-everything-privacy-vs-convenience-is-dividing-condos/2595465/> accessed 8 July 2026

Kodali S, 'Ten Reasons Why the Digital Personal Data Protection Bill Won't Empower the Public' *The Wire* (7 August 2023) <https://thewire.in/law/will-the-data-protection-law-empower-the-public> accessed 3 July 2026

McMullan T, 'What Does the Panopticon Mean in the Age of Digital Surveillance?' *The Guardian* (London, 23 July 2015)

Tripathi V, 'MyGate Advertising – Types, Ad Targeting & Facts' (*The Media Ant*, 8 June 2023) <https://www.themediaant.com/blog/mygate-advertising-types-and-audience-targeting/> accessed 8 July 2026

Websites and Blogs

Kamesh, 'The Nth Order Effect: MyGate's Early Approvals Impact on Last-Mile Delivery ETA' (*The Product Town*, 8 January 2025) <https://theproducttown.substack.com/p/the-nth-order-effect-mygates-early> accessed 8 July 2026

Paul I A, 'Are Prisons Computers?' (*ianalanpaul.com*) <https://www.ianalanpaul.com> accessed 25 June 2026

Other

Roti Kapada Aur Makaan (Manoj Kumar Productions 1974)