International Journal of
Global Multidisciplinary Research and Analytics

IJGMRA | ISSN (Online): 3107-6483
July-September 2025 | Vol. 01 | Issue 2

Website: www.thearyapublication.com

Beyond Access: Toward a Feminist Infrastructural Theory of Digital Citizenship and Gendered Risk in Contemporary India

[1]Mahera Imam & Dr. Ajay Sharma Chinnadurai[2]

[1]Research Scholar, Department of Women's Studies, Khajamalai Campus, Bharathidasan University, Tiruchirappalli, Tamil Nadu-620023
[2]Assistant Professor, Department of Political Science, Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam, Tiruchengode – 63720.
E-Mail:
DOI: http://doi.org/10.5281/zenodo.17312918

Accepted on: 28/09/2025 Published on: 10/10/2025

Abstract:

"Development can be seen as a process of expanding the real freedoms that people enjoy."
Amartya Sen

This paper contends that treating "access" as the endpoint of digital inclusion obscures the infrastructural arrangements that (re)produce gendered exclusions and risks in India. Building on feminist STS and information-infrastructure studies Susan Leigh Star and Geoffrey Bowker's insight that infrastructures are relational and embed power; Judy Wajcman's techno-feminism; Safiya Noble's account of algorithmic oppression; Ruha Benjamin's critique of carceral techno-politics; and Naila Kabeer's agency-capability lens we reconceptualize digital citizenship as an infrastructural condition rather than an individual attribute. We propose a Feminist Infrastructural Theory (FIT) operationalized through a 5A+S heuristic Availability, Affordability, Ability, Agency, and Assurance/Safety to explain why connectivity alone does not translate into voice, rights, or safety online. Using recent secondary evidence (global mobile-internet gender gaps; India's NFHS-5 on internet use; administrative cybercrime statistics), we show both progress and persistent disparities. Foundational inequalities in basic use align with education, income, and geography, while affordability shocks, skills gaps, patriarchal norms, and weak redressal pathways depress women's realized capabilities. Rising rates of online harassment, financial fraud, and image-based abuse indicate that Assurance/Safety must be treated as a precondition rather than a downstream outcome of meaningful participation. The paper contributes: (i) a testable framework (5A+S) to diagnose bottlenecks across sectors; (ii) an empirical map of India's gendered digital risks drawing on 2019–2025

datasets; and (iii) a policy-audit checklist that centers agency and safety shifting the evaluative question from "how many are connected?" to "who is protected, empowered, and able to exercise rights online?"

Keywords: *Feminist Infrastructural Theory (FIT), Digital Citizenship, Gender Digital Divide (India), 5A+S Heuristic, Technology-Facilitated Gender-Based Violence (TFGBV).*

1. Introduction:

India's twenty-first-century development story is often told through the idiom of digitization. Broadband expansion, low-cost data, mobile-first economies, biometric identity, and platformed governance have become the anchors of its state-building narrative. Flagship initiatives like Digital India have promised to knit citizens into a single informational fabric, while global development frameworks have increasingly stressed the role of ICTs in achieving the Sustainable Development Goals (SDGs). SDG-5 (gender equality), SDG-9 (industry, innovation, and infrastructure), and SDG-16 (peace, justice, and strong institutions) each contain explicit references to inclusive digital access, equitable participation, and strengthened governance. The vision is compelling: an India where connectivity enables women and marginalized communities to leap across structural barriers, exercise rights, and participate in public life on equal terms. Yet this triumphant discourse often mistakes access for inclusion. Policymakers count towers, SIM cards, and "active internet users" as though these metrics alone exhaust the meaning of digital citizenship. But feminist scholars of technology and infrastructure caution us that access is only the first rung on the ladder. What matters more is the infrastructural arrangement beneath the surface: who controls the device, who pays for recurring data, who has the skills to navigate platforms, whose speech is protected by governance systems, and who can realistically seek redress when harmed. When these infrastructures are absent or unevenly distributed, the very act of being connected may amplify existing inequalities, exposing women to new forms of risk rather than expanding freedoms. Infrastructures, as Susan Leigh Star observed, become visible precisely at the moment of breakdown and for women in India, these breakdowns occur daily in the form of dropped connections, shared handsets, language barriers, or failed grievance systems.

1.1.Digital Citizenship and Its Limits:

This paper contends that digital citizenship in India cannot be defined as mere connectivity. Rather, it must be reconceptualized as an infrastructural condition. Drawing on Amartya Sen's vision of development as the expansion of "real freedoms," the question is not simply whether women are online, but whether the digital environment expands their substantive capabilities: the ability to participate safely, to exercise voice, and to claim rights without disproportionate cost or risk. The normative benchmark is therefore higher than access it is capability with safety. Building on feminist science and technology studies (STS), we propose a Feminist Infrastructural Theory (FIT), operationalized through the 5A+S heuristic: Availability, Affordability, Ability, Agency, and Assurance/Safety. Each domain corresponds to a material or institutional condition that shapes whether connection becomes citizenship. Together, they expose how infrastructures reproduce gendered exclusions when treated as neutral backdrops rather than contested sites of power.

1.2. Why This Argument Matters Now

The urgency of moving "beyond access" is underlined by recent evidence from 2019–2025.

- **Global picture**. According to the International Telecommunication Union's Facts and Figures 2024, 70% of men and 65% of women worldwide used the internet leaving 189 million more men online than women. The global gender divide has narrowed in aggregate but widened in some of the least developed countries, underscoring how aggregate parity can mask deep regional disparities.
- **LMICs and South Asia.** In low- and middle-income countries, mobile remains the dominant gateway to the internet, yet GSMA's Mobile Gender Gap Report 2024/25 shows that women are still 15% less likely than men to use mobile internet. South Asia alone accounts for nearly 60% of women who remain unconnected, making it the epicentre of the global digital divide. In fact, South Asian women are over 40% less likely to use mobile internet compared to men a gap that has proven stubborn or even widened in some years, reflecting the compounded effect of affordability barriers, cultural norms, and safety concerns.
- **India's reality.** Within India, the National Family Health Survey-5 (2019–21) documents stark gaps: only 33% of women reported ever having used the internet, compared to 57% of men. These disparities intensify at lower wealth quintiles, among

rural households, and among women with less education. Crucially, "ever used" is a minimal threshold it does not capture regularity, autonomy, or safety of use. A woman who has once borrowed a handset to access WhatsApp is counted equally with one who navigates multiple platforms daily with full control of her device and data. Such measurement flattens the lived complexity of digital citizenship.

- **Rising cyber risks.** Simultaneously, digital harms are escalating. The National Crime Records Bureau reported a 31% rise in cybercrimes in 2023, with 86,420 cases nationwide. Offenses such as online harassment, financial fraud, identity theft, and non-consensual image circulation disproportionately affect women. Media coverage and independent feminist reports point to increasing withdrawal from online spaces, not due to lack of access but because of fear, fatigue, and failed redressal systems. This indicates that Assurance/Safety is not a downstream benefit but a precondition of sustained participation.

Taken together, these figures reveal a paradox. While India celebrates expanding connectivity, foundational inequalities persist and new risks proliferate. The binary of "connected/unconnected" conceals more than it reveals; what matters is the quality, control, and safety of participation. Without infrastructures that support affordability, ability, agency, and assurance, the digital realm risks becoming another arena of exclusion.

Purpose and Contribution:

This study seeks to reframe the debate by advancing Feminist Infrastructural Theory (FIT) and the 5A+S heuristic. Instead of asking "how many are online?", we ask: "who is protected, empowered, and able to exercise rights online?" Specifically, the paper makes three contributions:

1. **Conceptual framework**. FIT with 5A+S offers a testable, feminist diagnostic for analysing digital citizenship as an infrastructural condition.
2. **Empirical mapping.** By synthesizing secondary data from ITU, GSMA, NFHS-5, NCRB, and UN Women's SDG reports, we chart India's gendered digital landscape between 2019 and 2025.

3. **Policy tool.** We propose a policy-audit checklist that centers agency and safety, enabling governments, platforms, and civil society to evaluate infrastructures not merely by coverage but by their capacity to expand freedoms.

India's digital transformation presents both an opportunity and a warning. Opportunity, because inclusive infrastructures can catalyse gender justice and development. Warning, because equating connectivity with citizenship risks legitimizing fragile, unsafe participation that leaves structural inequalities untouched. The remainder of the paper builds out this argument: first by tracing theoretical foundations in feminist STS and digital governance, then by articulating the FIT model with its 5A+S dimensions, before turning to empirical patterns and policy pathways.

Roadmap: The paper proceeds in four moves. Section 2 develops the conceptual scaffolding feminist STS, techno-feminism, data feminism, and capabilities reframing digital citizenship as an infrastructural condition. Section 3 presents the Feminist Infrastructural Theory (FIT) and the 5A+S heuristic (Availability, Affordability, Ability, Agency, Assurance/Safety, with Intersectionality) as a testable diagnostic. Section 4 details our methods and synthesizes 2019–2025 secondary evidence (ITU, GSMA, UN Women, NFHS-5, NCRB), then maps India's empirical landscape: use gaps by wealth/education/place and a risk topography that underscores safety as a precondition. Sections 5–7 translate findings into sectoral vignettes (education, work/gig, health, civic grievance) and a governance analysis (IT Act/Rules, DPDP 2023; GDPR/DSA comparators. Section 8 notes limitations and future research; Section 9 concludes by pivoting metrics from "connected" to "protected + empowered."

2. Conceptual & Theoretical Foundations

2.1 Feminist political economy of technology

A feminist political-economy lens foregrounds how digital systems are embedded in relations of social reproduction, distribution, and power. Nancy Fraser's account of capitalism's "hidden abodes" highlights how markets depend on under-recognized infrastructures of care and reproductive labour. Applied to the digital sphere, her redistribution/recognition/representation triad clarifies why expanding connectivity (a distributive good) does not translate into equal participation when care burdens and political voice remain uneven. Silvia Federici's work on

reproductive labour further explains how time poverty, unpaid care, and mobility constraints shape women's practical opportunities to learn, explore, and take risks online. When platform use is squeezed between domestic responsibilities, the space for skill acquisition and experimentation narrows; "adoption" becomes fragile and reversible. Critical scholarship on data and algorithms complements this macro view by locating harm inside information architectures themselves. Safiya Noble shows how search and ranking systems can encode stereotypes, while Ruha Benjamin theorizes "the New Jim Code," where ostensibly neutral optimizations reproduce stratification. These insights specify mechanisms through which gender and intersectional hierarchies are sedimented: from abusive autocomplete and ad targeting to content moderation asymmetries that differentially expose users to risk or silence their speech.

Shoshana Zuboff's analysis of surveillance capitalism adds the political-economic incentives that drive these technical outcomes: platforms profit from rendering behaviours legible and predictable, rewarding designs that maximize extraction and engagement even when those designs raise exposure to harassment, profiling, or coercive nudging. In low-resource settings, these dynamics intersect with affordability pressures (e.g., zero-rating and bundled apps), pushing first-time users into closed ecosystems where defaults are hard to change, consent is thin, and data externalities are opaque.

Taken together, feminist political economy reframes "access" not as a final state but as a contested relation co-produced by domestic labour regimes, market incentives, and technical systems. This sets up the need for an infrastructural account that can track how those relations become durable in practice.

2.2 Infrastructure studies

Infrastructure studies supply the vocabulary to analyse durability, maintenance, and failure. Bowker and Star famously argue that infrastructure is "by design" invisible, becoming perceptible at moments of breakdown. For gendered digital participation, breakdowns are diagnostic: unaffordable data, a lost password controlled by a family member, an abusive message with no accessible reporting channel, or a SIM registered to someone else's name. Each "glitch" reveals the standards, classifications, and handoffs that ordinarily remain out of sight.

Brian Larkin pushes further, emphasizing the aesthetics and politics of infrastructure how cables, towers, IDs, and interfaces materialize state and corporate power, and how their presence/absence redistributes possibilities. In the Indian context, think of KYC norms for SIM registration, handset repair markets, or vernacular font support: each is a site where capability is quietly enabled or foreclosed.

Standards and governance sit at the core of this perspective. Protocols (from spectrum allocation and SIM registration to API policies and default privacy settings) are normative settlements: they choose whose labour counts (e.g., who must do the work of grievance filing), which harms are legible, and what forms of identity are recognized. Because infrastructures are path-dependent and capital-intensive, early design choices persist; even small asymmetries like default public profiles or high-friction reporting can compound over time into predictable gendered risks.

An infrastructural approach therefore urges us to look across layer's devices, networks, platforms, institutions rather than isolating a single node. It also insists that measurement include not only roll-out (towers installed, kilometres of fibre) but maintenance and repair: whether abused accounts are restored, whether grievance windows are open when users are free, whether language interfaces match literacy practices, whether protective defaults are on by default for vulnerable users.

2.3 Digital citizenship & safety

"Digital citizenship" is often invoked as a rights-inflected ideal access to information, expression, association, and redress in networked publics. A rights-based approach centres due process (clear rules, notice, appeal), equality (non-discrimination, accessibility), and privacy (data minimization, purpose limitation) as preconditions for meaningful participation, not optional add-ons.

The literature on technology-facilitated gender-based violence (TFGBV) details how harassment, doxxing, non-consensual image distribution, and cyberstalking generate chilling effects users restrict speech, adopt self-censoring behaviours, or exit platforms. These behavioural adaptations link directly to the citizenship agenda: when some groups must pay

"safety taxes" (time, emotional energy, device duplication, legal fees) to remain online, formal rights are hollowed out in practice.

Intersectionality, following Kimberlé Crenshaw, cautions against treating "women" as a unitary subject. Risks and capabilities are mediated by caste, class, region, age, language, disability, and occupation. For instance, the same content-moderation rule can protect one group while over-policing another; the same privacy setting can be trivial for those with private rooms and multiple devices, yet critical for those sharing phones or subject to household surveillance.

Donna Haraway's cyborg politics helps name the hybridity of online/offline selves and the permeability of boundaries useful for understanding how constraints on bodily mobility, care responsibilities, or reputational risk travel into digital decisions. Catherine D'Ignazio and Lauren Klein's "data feminism" then operationalizes this stance into design and governance: shift from "fixing" women to interrogating power; value situated knowledge; examine how default categories (real-name policies, binary gender fields, ID requirements) enact exclusions; and redistribute the labour of safety away from victims and toward institutions with capacity.

Definitions

- **Access**: Physical and economic connection to digital networks and devices (coverage, device availability, subscriptions, and recurring costs). In this paper, access is necessary but not sufficient for participation.
- **Capability**: The substantive freedom to achieve valued digital functioning's (learning, working, organizing, care-seeking, leisure). Draws on capability approaches: focus on what people can actually do, not just what they theoretically could do.
- **Agency**: The power to decide whether, when, and how to use technologies control over accounts, passwords, time, and content; freedom from coercion in digital choices. Agency includes intra-household, workplace, and community bargaining.
- **Assurance/Safety**: The expectation and experience of protection from harm (harassment, surveillance, coerced exposure), plus accessible redress when harm occurs (reporting, support services, due process). Assurance is treated as a precondition for sustained participation.

- **Digital citizenship**: The enjoyment and exercise of rights, protections, and responsibilities in networked environments spanning expression, association, access to information, privacy, and remedy such that individuals can participate without disproportionate risk.
- **TFGBV (Technology-Facilitated Gender-Based Violence)**: Harms that are enabled, amplified, or sustained through digital technologies, including harassment, cyberstalking, doxxing, extortion, non-consensual image distribution, impersonation, and targeted disinformation. TFGBV includes both online acts and offline impacts (withdrawal from platforms, reputational damage, employment loss, mental health effects).

2.4 Feminist STS & Infrastructure Studies

A feminist reading of science and technology studies (STS) insists that infrastructures are not neutral utilities but deeply political arrangements. Susan Leigh Star, in her seminal work with Karen Ruhleder and Geoffrey Bowker, defined infrastructures as relational, embedded, and power-laden. They remain invisible when functioning smoothly but become acutely visible at the point of breakdown. This insight reframes the digital divide: a woman's device may technically connect her to a network, but the moment she cannot afford the next data recharge, or when her complaint about online abuse goes unanswered, the infrastructure of inclusion is revealed as fragile and exclusionary. Star and Bowker remind us that infrastructure is always a site of social ordering decisions about what to standardize, whose needs to prioritize, and what forms of breakdown are tolerated reflect embedded hierarchies of power. This approach helps us move "beyond access." Mere coverage maps or user counts cannot capture the lived realities of participation. Instead, we must ask: under what infrastructural arrangements does digital citizenship become possible, and for whom does it fail? Feminist STS demands that we situate digital inclusion in the messy entanglements of devices, tariffs, skills, identities, and grievance systems rather than in binary categories of connected/unconnected.

- Judy Wajcman's techno-feminism extends this argument by emphasizing the co-production of gender and technology. Technologies are not neutral tools applied to pre-existing subjects; rather, they are shaped by social relations even as they shape them in return. Mobile phones in India, for example, were heralded as liberatory tools for

women, yet the ecosystem of affordability, patriarchal household surveillance, and device-sharing has reinforced women's dependence rather than autonomy in many cases. Watchman's insight is that gender hierarchies and technical designs evolve together: the "normal" user imagined by handset designers or platform engineers often maps onto male, literate, urban, and financially autonomous actors, leaving women and marginalized communities as perpetual "others." By reading infrastructures through techno-feminism, we see how digital systems consolidate, rather than disrupt, patriarchal social orders unless explicitly challenged.

- Safiya Umoja Noble and Ruha Benjamin take us deeper into the digital core, revealing how algorithmic and data infrastructures can reproduce structural inequalities. Noble's Algorithms of Oppression demonstrates how search engines amplify racist and sexist stereotypes, embedding bias in seemingly neutral systems. For women in India, whose digital footprints are often mediated through English-language platforms and global advertising logics, these algorithmic architectures can invisibly distort visibility, voice, and credibility. Benjamin's work on carceral technoscience extends this critique, showing how surveillance, risk prediction, and automated decision-making often replicate racial and gender hierarchies under the guise of efficiency. In the Indian context, the proliferation of biometric identity (Aadhaar), platformed welfare, and AI-driven fraud detection risks amplifying exclusion for women who lack documentation, financial independence, or institutional trust. Noble and Benjamin remind us that the harms women face online are not aberrations they are features of infrastructures designed without feminist accountability.
- If Noble and Benjamin expose algorithmic harms, Catherine D'Ignazio and Lauren Klein's Data Feminism challenges us to rethink data practices themselves. They argue that data is never raw; it is always structured by power. Feminist data practices therefore require us to ask: who is counted as a user? whose experiences of harm are made visible? whose silences are misread as absence? For instance, India's NFHS-5 survey measures "ever used the internet" but tells us little about whether women's use is regular, autonomous, or safe. From a data feminist lens, such indicators flatten inequality, treating fleeting or coerced access as equivalent to meaningful participation. Data Feminism insists on designing power-aware indicators such as private device

control, confidence in using safety features, or time-to-redress after reporting abuse that can capture the lived conditions of digital citizenship.

- Nancy Fraser provides a broader normative framework by arguing that justice requires attention to redistribution, recognition, and representation. Applied to digital infrastructures, redistribution speaks to Affordability: ensuring women are not priced out of sustained and safe digital use. Recognition aligns with Ability and Assurance: valuing women lived experiences, ensuring platforms acknowledge harms, and embedding cultural and linguistic inclusivity into design. Representation is closest to Agency: women's voice in shaping the rules of platforms, the governance of algorithms, and the policy frameworks of digital states. Fraser's tripartite model allows us to map the terrain of feminist infrastructural justice and highlights that inclusion requires structural transformation across economic, cultural, and political dimensions.
- Finally, the work of Naila Kabeer and Amartya Sen anchors this conceptual terrain in the capabilities and agency tradition. Sen famously argued that development is the expansion of real freedoms not just the provision of resources, but the actual opportunities to do and be what people value. Kabeer elaborates on this in gendered contexts, showing how agency is not a binary possession but a situated capacity, contingent on social norms, resources, and institutions. Applied to digital infrastructures, this means that a SIM card, a handset, or a free data pack are not themselves markers of citizenship. The relevant question is whether a woman can actually use these tools to pursue valued goals without disproportionate risk. Does she have the autonomy to keep her device private? Can she participate in online education without surveillance? Can she report abuse and expect timely redress? Can she access work opportunities online without harassment or fraud? Capabilities thinking shifts the focus from inputs (access, devices) to functioning and freedoms the substantive outcomes of digital life.

Taken together, these theoretical foundations converge on a powerful proposition: digital citizenship is not an individual attribute but an infrastructural condition. Infrastructures of pricing, devices, skills, platforms, and redressal systems are relational, gendered, and power-laden. Feminist STS helps us see breakdowns as windows into embedded hierarchies; techno-feminism reveals co-production between gender and technology; algorithmic critiques show

how bias is baked into data architectures; data feminism urges power-aware indicators; Fraser provides the justice framework; and Sen and Kabeer offer the evaluative lens of capabilities and agency. This conceptual synthesis forms the basis of the Feminist Infrastructural Theory (FIT) that guides the paper. FIT's analytical grammar, distilled into the 5A+S heuristic Availability, Affordability, Ability, Agency, and Assurance/Safety translates these theoretical insights into diagnostic domains. Each domain is simultaneously empirical (measurable with indicators), normative (linked to justice), and practical (actionable through policy and design). The following sections build on this foundation, applying FIT to India's digital landscape between 2019 and 2025 to show how infrastructures enable or foreclose women's substantive freedoms online.

3.Methodology

This study adopts a secondary-evidence synthesis (2019–2025), reading India's gendered digital participation through the FIT–5A+S lens (Availability, Affordability, Ability, Agency, Assurance/Safety, with Intersectionality throughout). We harmonize publicly available indicators and definitions from ITU Facts & Figures 2024 (global use/parity), GSMA Mobile Gender Gap 2024/25 (LMIC/South Asia access, affordability and barriers), UN Women Gender Snapshot 2024/25 (SDG framing), NFHS-5, 2019–21 (sex-, wealth-, education-, and residence-disaggregated internet use), and NCRB Crime in India 2023 (cybercrime levels/categories). For each domain, we align proxies e.g., private device control and continuity of use (Availability), total cost of ownership relative to women's incomes (Affordability), task-based and self-efficacy cues such as privacy settings or account recovery (Ability), autonomy over device/identity and context of use (Agency), and exposure/redress patterns for TFGBV and related harms (Assurance). Recognizing limits NFHS-5's "ever used" is a low bar; NCRB reflects reported, not total, harms; GSMA is mobile-centric we privilege converging signals across sources and flag priority gaps (direct agency/redress measures, intersectional disaggregation) for future monitoring.

4. Empirical Landscape: India 2019–2025

4.1 Use & Gaps: What "Access" Hides

The most widely cited national statistic NFHS-5 (2019–21) reports that 33% of women and 57% of men in India have ever used the internet. This headline already signals a foundational divide, but its real force emerges once we cut the data by wealth, education, and residence.

Wealth gradient. Internet use climbs sharply with household wealth. Women in the lowest quintile report substantially lower use than those in the highest; men display the same pattern but start from a higher base. This gradient functions as a proxy for affordability: higher TCO (device purchase/repair + data) relative to income depresses sustained participation. Crucially, affordability shortfalls often translate into device sharing and intermittent usage, conditions that erode privacy and reduce opportunities for skill acquisition.

Education gradient. Education is the strongest single correlate of women's internet use. Among women with no schooling, reported use is extremely low; among college-educated women, it is the norm. Education is not merely a skills proxy—it also shifts aspirations, confidence, and bargaining power, supporting the Ability and Agency domains in tandem. The implication is straightforward: capability-building interventions (language localization, task-based digital and safety literacy) are as essential as network expansion.

Urban–rural divide. Urban women's reported use substantially exceeds rural women's, reflecting not only Availability (denser coverage, better handset markets) but also Affordability (higher and steadier incomes) and Agency (more permissive norms for independent phone use). Yet urban averages conceal pockets of precarious inclusion: low-income urban women may still ration data, rely on shared devices, or work in settings were employer surveillance and BYOD policies compromise autonomy.

Together, these cuts reveal a consistent pattern: headline access undercounts infrastructural scarcity. Even where coverage exists, private device control, affordability stability, and safety know-how determine whether connection becomes durable capability. In other words, the gender gap is not only a gap of entry but a gap of conditions.

4.2 Risk Topography: Why Safety Is a Precondition

If access metrics describe the front door, risk metrics describe what happens once inside. NCRB (2023) recorded a 31% year-on-year rise in cybercrimes (86,000 cases nationally). While NCRB categorizations evolve, the persistent picture is clear: online harassment, financial fraud,

identity theft, and image-based abuse form a growing share of reported harms with gendered impacts.

Three features of the risk landscape stand out:

1. **Scale meets exposure.** As payments, commerce, education, and services digitize, women's necessary exposure to platforms and messaging ecosystems increases. Without commensurate strengthening of Assurance infrastructures clear reporting flows, local-language moderation capacity, survivorship-centered evidence norms incidents escalate from isolated events into durable exclusions (withdrawal, self-censorship, avoidance of opportunities).
2. **Latency of redress.** Even where reporting occurs, time-to-acknowledge and time-to-action can be long, and outcome transparency thin. Requirements like original device files or uncompressed media may be procedurally neutral yet structurally exclusionary for women using shared/low-end devices who cannot safely store evidence. Slow or opaque redress turns the cost–benefit calculus against participation.
3. **Visibility bias.** Reported cases likely undercount prevalence, especially for non-consensual image circulation and cyberstalking, where stigma and fear of retaliation are high. Consequently, observed increases can reflect both real growth and improved reporting but either way, they underscore that safety is a prerequisite for sustained participation.

4.3 Reading India Through 5A+S

Availability. India's supply-side gains (coverage expansion, falling average data prices) coexist with control deficits: many women still rely on shared devices and constrained spaces of use. Globally, ITU 2024 shows 70% of men vs 65% of women online, leaving 189 million more men connected. The parity headline masks regional fragility, a caution that simple coverage indicators are insufficient to infer capability.

Affordability. GSMA 2024/25 finds women in LMICs 15% less likely to use mobile internet, with South Asia accounting for a disproportionate share of the unconnected. In practice, women in India face lumpy costs (handset purchase/repair) and recurring costs (recharges) that are

difficult to smooth with irregular earnings. Affordability shortfalls drive risky workarounds: borrowed phones, public Wi-Fi, or compromised app permissions that trade safety for utility.

Ability. The education gradient in NFHS-5 implies large skills and confidence gaps. Beyond functional tasks, safety literacy (privacy settings, blocking/reporting, safe evidence captures) is thinly measured yet central to conversion of access into capability.

Agency. Autonomy over identity, device, and time of use remains constrained by intra-household norms and workplace controls (e.g., monitoring apps, identity mandates). Agency deficits are the least measured elements in current surveys, creating a blind spot: women's "use" can rise while their freedom to choose how and under what identity to use remains curtailed.

Assurance/Safety. Rising NCRB counts and persistent reports of harassment and IBA demonstrate that harms are neither rare nor easily remedied. Where platform moderation lacks local-language capacity and police cyber cells are unevenly staffed, victims bear private costs (time, money, stigma) for public failures of assurance.

Intersectionality. The wealth and education cuts in NFHS-5 show steep stratification; rural residence and youth (especially adolescent girls) add further constraints. Although nationally representative data on caste and disability in digital participation are limited, qualitative and sectoral studies indicate compounded exclusion for Dalit, Adivasi, and disabled women via device scarcity, connectivity gaps, and disproportionate exposure to online abuse.

4.4 What the Patterns Mean

Three implications follow.

First, access metrics overstate inclusion. "Ever used" cannot stand in for regular, autonomous, and safe participation. Upgrading monitoring to capability and safety indicators private device control; frequency/continuity of use; safety literacy; time-to-redress—would align India's dashboards with the reality's women face.

Second, safety determines sustainability. As online dependence grows, Assurance moves from "nice to have" to precondition. Statutory service-level targets for platform response, survivor-

centred evidence protocols, and interoperable takedown/de-indexing mechanisms would materially change the cost calculus of participation for women.

Third, intersectional targeting is essential. If the steepest deficits cluster at the intersection of female × rural × poorest quintile × low education, then device finance, data allowances, and safety-literacy programs must be place-based and cohort-specific, co-designed with local women's groups to ensure uptake and trust.

India's 2019–2025 trajectory shows genuine progress alongside structural bottlenecks. Read through 5A+S, the evidence suggests that availability gains will not mature into capabilities and freedoms without affordability stability, skill/confidence pipelines, agency-preserving design, and reliable assurance systems attentive to the intersectional realities that shape women's digital lives.

5. Sectoral Vignettes

5.1 Education & Skilling (Ability, Affordability)

India's education digitization from DIKSHA repositories to university LMS platforms often presumes a frictionless learner. In reality, ability and affordability jointly govern whether a girl or young woman can stay the course. Where schools rely on WhatsApp homework, shared devices collapse the boundary between study and household surveillance; where video lectures are the default, data costs punish those in prepaid, low-income plans. Ability is not only app literacy; it includes safety know-how (configuring group privacy, muting unknown callers, reporting harassment) and confidence to troubleshoot without male "permission." Financially, the total cost of ownership (TCO) a basic smartphone, data, earphones, repairs can exceed monthly discretionary income, producing rationing (e.g., avoiding live classes to save data) that quietly compounds learning gaps. Programs that pair women-first device finance with micro-learning safety modules (privacy settings, account recovery, evidence capture) convert bare access into capability. In short: whenever curricula assume continuous, private, and safe connectivity, ability and affordability must be funded as core learning infrastructure, not left to households.

5.2 Work & the Gig Economy (Agency, Assurance)

Platformed work delivery, care, beauty services, micro-tasks offers flexible entry points but imports agency and assurance dilemmas. Agency frays when onboarding requires real-name display, public profile photos, or GPS trail visibility that exposes women to doxxing or offline harassment. BYOD (bring-your-own-device) policies can bleed employer control into the private sphere via monitoring apps, location pings after hours, and forced biometric logins. Assurance deficits show up when in-app reporting produces templated replies, when evidence rules reject screenshots from low-end phones, or when ratings systems amplify retaliation. A feminist infrastructural stance implies: (i) pseudonymous display layers where safety risks are high; (ii) separation of identity proofs from public presentation; (iii) statutory SLAs for incident response; and (iv) joint liability regimes in which platforms share responsibility for harms occurring in the ordinary course of platform-mediated work. When agency and assurance improve, women's participation rises not only in numbers but in quality higher-value tasks, greater voice, and lower churn.

5.3 Health/Telemedicine (Availability, Ability)

Telemedicine promises reach across India's geography, yet availability and ability shape whether it delivers for women. Clinic video calls and e-prescriptions presume uninterrupted signal, a quiet room, and a private device condition often unavailable to women juggling care work in crowded homes. Where a spouse or in-law owns the phone, intimate privacy becomes speculative; sensitive consultations (mental health, reproductive care) may be impossible. Ability combines digital and health literacies: navigating app interfaces, managing consent for data sharing, and understanding pharmacy fulfilment flows. Policy and design responses include low-bandwidth audio-first options, privacy-preserving appointment flows (alias names on notifications, one-tap "hide" modes), and front-loaded consent cues that clarify what data move to whom. Making private device control a criterion in health outreach (e.g., device grants tied to ASHA-linked programs) treats availability as a public health input rather than a family's discretionary spend.

5.4 Civic Participation & Grievance (Agency, Safety)

From ration claims to municipal complaints to women's helpline apps, civic tech presumes that form-filling equals voice. But agency hinges on whether women can speak without retaliation (pseudonymity, shielded contact details) and whether grievance systems acknowledge, act, and

explain. Safety failures doxxing after filing, leaky dashboards exposing phone numbers, call-backs scheduled during family time convert participation into risk. A rights-respecting design offers: (i) masked identities visible to officials but not to the public; (ii) status-tracked tickets with human-readable reasons for decisions; (iii) appeal lanes independent of the initial decision-maker; and (iv) language localization beyond interface strings (scripts, IVR hotlines, WhatsApp bots). When civic platforms meet these barometers, women's online claims-making ceases to be episodic and becomes durable citizenship.

6. Governance & Policy Landscape

6.1 India's Regulatory Stack: IT Act, IT Rules, DPDP Act 2023

India's digital rulebook is anchored in the Information Technology Act, 2000, supplemented by the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and subsequent amendments, and the Digital Personal Data Protection Act, 2023 (DPDP). Together, they define platform obligations, user reporting pathways, and data fiduciary duties.

- **IT Act & IT Rules.** Intermediaries must publish rules, appoint grievance officers, and remove unlawful content upon actual knowledge/notice. For women's safety, this creates hooks for reporting and takedown, but two chronic gaps persist: (i) service-level expectations (time-to-acknowledge/action) are weakly specified and unevenly enforced; (ii) language capacity for moderation and support lags India's linguistic diversity, delaying relief where harms escalate fastest.
- **DPDP Act, 2023.** The Act reframes entities as Data Fiduciaries with duties of purpose limitation, notice/consent, data subject rights (access, correction, erasure), and grievance redress. For gender safety, DPDP's promise lies in consent clarity, children's protections, and a formal Data Protection Board. The gaps: functioning timelines, women-first consent UX (readability, local languages), and clear redress escalation from platforms to the Board for privacy harms intersecting with TFGBV (e.g., non-consensual image circulation).

Policy opportunity: Treat platform Grievance Officers and DPDP-mandated redress as a joined safety fabric: common incident taxonomies, time-bound SLA tiers (24h

acknowledgment; staged actions), survivor-centered evidence rules (accepting screenshots, chat exports), and coordinated de-indexing across search and social media.

6.2 Global Comparators: GDPR and EU DSA

Two European frameworks offer conceptual bearings:

- **GDPR** centres lawfulness, fairness, transparency, data minimization, and Data Protection Impact Assessments (DPIAs) for high-risk processing. A feminist read emphasizes DPIAs as tools for intersectional risk assessment (e.g., harms to women using shared devices; coercive consent in households; re-identification risks in small communities).
- The **EU Digital Services Act (DSA)** imposes systemic risk assessments on large platforms (VLOPs), mandates notice-and-action, appeals, and audits of recommender systems. For India's context, the DSA's structure suggests codifying risk-of-gendered harm as a category in platform risk reports; requiring public dashboards on response times; and enabling independent audits of moderation and recommendation impacts in Indian languages.

Adaptation logic: Rather than importing regimes wholesale, India can operationalize home-grown, audit-ready barometers aligned with FIT: availability (device control), affordability (TCO), ability (safety literacy), agency (identity choice & consent), assurance (time-bound redress). Embedding these into licensing conditions, tender criteria for public platforms, and **voluntary codes with teeth** brings comparators to life in local law-and-practice.

6.3 Normative Anchor: SDGs + Feminist Digital Justice

SDG-5 (gender equality), SDG-9 (resilient infrastructure), and SDG-16 (access to justice) together suggest that infrastructure and justice are co-produced. A feminist digital-justice lens adds: (i) redistribution subsidies and fair pricing to ensure affordability; (ii) recognition interfaces, languages, and support that respect lived realities; and (iii) representation women's voice in standard-setting and oversight. The governance test, then, is not compliance on paper but capability with safety in practice.

7. Discussion

This paper's central claim is that assurance/safety is a precondition, not an afterthought, of digital participation. The evidence is practical: when redress stalls or fails, women withdraw, self-censor, or revert to shared/risky use nullifying gains in access. In FIT terms, Assurance stabilizes the other A's: without it, affordability investments leak (wasted data, duplicate devices after account compromise), availability brittle (avoidance during high-risk hours), ability unused (learned helplessness after failed reports), and agency curtailed (silence to avoid retaliation).

Fraser's three-dimensional justice clarifies the design agenda. Redistribution demands that pricing and device ecosystems recognize women's income patterns credit for low-documentation workers; device trade-ins; public data allowances earmarked for safety-critical services (helplines, grievance portals, learning platforms). Recognition requires power-aware design: local-language moderation, survivor-centered evidence rules, and interfaces that assume shared devices (stealth modes, masked notifications). Representation means women must shape the rules advisory councils with decision weight, annual public audits of platform risks in Indian languages, and transparent appeals with reasons.

These principles travel across the stack. Telecom regulation can treat "private device control for women" and "data-rationing days" as universal service outcomes. Platform policy can shift defaults: safer privacy settings at install, context-dependent friction for contact from unknowns, and choice architectures that privilege wellbeing over engagement. State platforms can publish SLA dashboards on grievance timelines, localize assistance via IVR and WhatsApp, and protect complainant identities by default. Civil society can co-produce safety literacy that goes beyond how-to tips to right-claiming scripts: how to document, escalate, and invoke statutory obligations.

The implications for feminist digital citizenship are direct. Citizenship is not a login; it is the capability to appear, speak, organize, and refuse in digital spaces without disproportionate cost or danger. The move from "connected" to "protected + empowered" requires outcome metrics aligned with lived realities. Counting "active users" should give way to tracking time-to-redress, appeal success, de-indexing coverage after image-based abuse, private device control, and confidence to report. When those measures improve especially for the poorest rural women and for adolescent girls' digital citizenship thickens from access to freedom in practice.

Finally, FIT explains why progress feels uneven. A program can distribute millions of SIMs yet leave women exposed if platforms lack local moderation. Data prices can fall yet affordability worsen if wages stagnate or repair costs spike. Skills trainings can proliferate yet fail if women cannot exercise agency over identity or if household surveillance punishes learned competence. FIT's value is to see the system: upgrading one domain rarely suffices; synchronized improvements across the A's are what convert connection into durable capability.

8. Limitations & Future Research

This study synthesizes secondary data (2019–2025) to diagnose gendered digital participation through FIT. Several limitations qualify the findings. First, NFHS-5's "ever used the internet" is a low threshold that cannot distinguish frequency, autonomy, or safety. Without direct measures of private device control, shared use, and continuity, capability is likely over-estimated. Second, NCRB crime statistics track reported cases, shaped by stigma, awareness, and policing capacity; category changes and uneven state reporting complicate comparisons over time. Third, GSMA barrier modules are mobile-centric, potentially undercounting multi-device ecologies (feature phones + shared smartphones + cybercafés). Fourth, nationally representative data are sparse on caste, disability, and marital status in relation to digital harms, limiting a fully intersectional map.

Future work should therefore pursue mixed methods. On the quantitative side: (i) task-based capability metrics (privacy configuration, account recovery, reporting navigation); (ii) device-control inventories (solo vs shared, lock practices); (iii) redress performance (time-to-acknowledge/action, appeal outcomes); and (iv) intersectional disaggregation by caste, region, age, disability. On the qualitative side: digital ethnographies of household bargaining, workplace surveillance spillovers, and survivor journeys through grievance systems. A participatory approach co-designing a FIT scorecard with women's organizations, helplines, and platform teams can validate indicators, surface hidden frictions, and set locally credible targets. Finally, linking administrative data (helpline logs, platform transparency reports) with survey measures would enable triangulation between exposure, reporting, and outcomes. Together, these upgrades would turn FIT from a diagnostic into a monitoring architecture for feminist digital justice.

9. Conclusion

This paper has argued that those freedoms are infrastructural. Counting connections without auditing the infrastructures that convert connection into capability with safety mistakes a doorway for a destination. Drawing on feminist STS and allied traditions, we proposed Feminist Infrastructural Theory (FIT) operationalized via 5A+S—Availability, Affordability, Ability, Agency, and Assurance/Safety, with Intersectionality throughout. Read against 2019–2025 evidence, FIT explains India's paradox: real gains in coverage and uptake alongside structural bottlenecks that depress women's realized capabilities and expose them to escalating digital harms. The contributions are threefold: a conceptual reframing (citizenship as an infrastructural condition), a diagnostic grammar (5A+S) to locate bottlenecks, and a policy-audit checklist that refocuses measurement from "how many are online" to who is protected, empowered, and able to exercise rights online. The governance corollary is clear: Assurance is not a downstream service but a precondition of sustained participation; Agency is not a luxury but the hinge of meaningful choice; Ability is safety literacy as much as app fluency; Affordability is redistributive policy; Availability is private, stable, and context-fit access—not just a tower on a map. Reorienting metrics to these realities' private device control, TCO relative to women's incomes, task-based safety skills, identity choice, and time-bound redress will align India's digital transformation with its SDG promise. The evaluative pivot is simple to state and demanding to realize: from connected to protected + empowered. Only then does digital citizenship in contemporary India approach Sen's vision freedom in practice, not merely connectivity in principle.

Acknowledgement:

I am deeply honored to have been awarded a Doctoral Fellowship by the Indian Council of Social Science Research (ICSSR). This publication is an outcome of ICSSR-sponsored doctoral research. However, I bear sole responsibility for the information presented, the views expressed, and the findings of this study. I am sincerely grateful to the ICSSR, Ministry of Education, Government of India, New Delhi, for their invaluable financial support, which made this work possible.

References:

- Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Polity.
- Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. MIT Press.
- D'Ignazio, C., & Klein, L. F. (2020). *Data feminism*. MIT Press.
- European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data… (General Data Protection Regulation).
- European Parliament and Council. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).
- Fraser, N. (1995). From redistribution to recognition? Dilemmas of justice in a "post-socialist" age. *New Left Review, 212*, 68–93.
- GSMA. (2024). *The mobile gender gap report 2024*. GSMA.
- Government of India. (2023). *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*. Gazette of India.
- International Institute for Population Sciences (IIPS), & ICF. (2021). *National Family Health Survey (NFHS-5), 2019–21: India—Fact sheets and report*. Ministry of Health and Family Welfare, Government of India.
- International Telecommunication Union. (2024). *Facts and figures 2024*. ITU.
- Kabeer, N. (1999). Resources, agency, achievements: Reflections on the measurement of women's empowerment. *Development and Change, 30*(3), 435–464.
- Ministry of Electronics and Information Technology. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (as amended in 2023).
- National Crime Records Bureau. (2024). *Crime in India 2023*. Ministry of Home Affairs, Government of India.
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.
- Sen, A. (1999). *Development as freedom*. Oxford University Press.
- Star, S. L., & Rohleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research, 7*(1), 111–134.
- UN Women, & United Nations Department of Economic and Social Affairs. (2024). *Progress on the Sustainable Development Goals: The gender snapshot 2024*. UN Women.