Security as Practice: User-Centered Data Protection under India's DPDP Act (2023–2025)

Adiba Saifi

ABSTRACT

India's Digital Personal Data Protection Act (DPDP, 2023–2025) represents a watershed moment in the country's evolving digital privacy landscape. This research provides a critical examination of the Act's legislative ambitions, practical implementation realities, and the persistent "user experience gap" that often transforms consent forms and terms of use from enablers of privacy into obstacles to meaningful engagement. Employing a dual-lens framework that integrates technical infrastructure considerations with human behavioral practices, the paper draws on original empirical survey data complemented by comprehensive policy analysis to reveal persistent gaps in user awareness, consent usability, and equitable access to digital privacy protections (Saifi, 2025).

The study synthesizes these insights with scholarly literature to propose actionable recommendations aimed at transforming data protection laws from abstract rights into everyday lived realities. Crucially, the research foregrounds the concept of "security as practice"—the understanding that privacy protection is not merely a legal or technological product but a dynamic, context-driven process shaped by the interplay of technical tools, institutional frameworks, and user behaviors (Schneier, 2000; Williams, 2020). Findings reveal that while the DPDP Act establishes a robust legal foundation, its transformative potential depends fundamentally on bridging the critical divide between formal protections and the lived experiences of diverse user populations. This research contributes to the broader understanding of how emerging digital governance frameworks can balance legal rigor, technological innovation, and user-centric design in diverse socio-cultural contexts, with particular relevance for other Global South nations navigating digital policy reform.

Key words: Digital privacy, data protection, self-directed security, DPDP Act, user experience, digital literacy, governance, India

INTRODUCTION

The rapid digital transformation of Indian society has introduced profound opportunities for economic participation, governance innovation, and social communication. Millions of Indian citizens now routinely access government portals, financial services, healthcare systems, and ubiquitous social media platforms, facilitating unprecedented connectivity and service delivery. Yet complementing these opportunities are significant challenges related to the safety, management, and ethical use of personal data. Across these diverse digital touchpoints, individuals routinely

share sensitive information—financial details, health records, biometric identifiers, location data, and behavioral profiles—creating an ever-growing trail of personal data vulnerable to misuse, unauthorized sharing, and breaches.

In response to these escalating risks and growing civil society advocacy, the Government of India enacted the Digital Personal Data Protection Act (DPDP) in August 2023, with substantive implementation rules introduced in 2025 (Government of India, 2023). The DPDP Act establishes a comprehensive legal regime defining the rights of "data principals" (individual users) and the obligations of "data fiduciaries" (organizations processing personal data). This legislation marks India's most ambitious statutory effort to regulate digital privacy to date, setting a clear legislative benchmark in South Asia's digital rights landscape. The Act mandates that consent for data processing must be obtained in a manner that is "free, specific, informed, unconditional, and unambiguous," thereby codifying layered privacy rights that echo and extend global best practices established by frameworks such as the European Union's General Data Protection Regulation (GDPR) (European Union, 2018).

Despite this strong legislative foundation, digital privacy remains a complex and often elusive goal for many Indian users. Beyond statutory provisions, the day-to-day experience of engaging with privacy notices, consent dialogues, and data management settings varies widely and often falls far short of the Act's aspirational vision. Confusing legal language, complex consent processes, and limited accessibility frequently impede users from making informed privacy decisions (AlZain et al., 2022; Bennett et al., 2020). This experiential gap is particularly acute in a multilingual, digitally unequal society where digital literacy and infrastructure vary markedly across regions, socioeconomic strata, and demographic groups. The persistence of this gap raises critical questions: How effectively can formal legal protections translate into meaningful user empowerment when many citizens lack awareness of their rights? How can institutions and organizations bridge the gap between legal mandates and user-centered implementation?

This paper therefore foregrounds the user experience within the discussion on digital privacy rights, seeking to uncover how the DPDP Act's legal ambitions translate—or fail to translate—into meaningful protections and empowerment for everyday users. Rather than treating privacy as a purely legal or technical matter, this study adopts the framework of "security as practice," which emphasizes that genuine privacy protection emerges through the dynamic integration of technical tools, legal literacy, institutional accountability, and culturally informed user behaviors (Schneier, 2000; Williams, 2020). This framing acknowledges that statutory rights alone are insufficient without parallel attention to the technical usability, organizational capacity, and social conditions that enable users to meaningfully exercise their rights.

The DPDP Act Explained: Rights, Rules, and Responsibilities

India's Digital Personal Data Protection Act embodies the most comprehensive statutory framework for digital privacy and personal data governance in Indian history (Government of India, 2023). The Act meticulously defines and formalizes the rights of "data principals"—the individual users—alongside the legally binding responsibilities of "data fiduciaries"—organizations and entities processing and managing personal data. At its core, the DPDP Act mandates that consent for data processing must be obtained in a manner that is "free, specific, informed, unconditional, and unambiguous," thereby codifying privacy protections that reflect evolving international standards in the digital rights domain (PRS Legislative Research, 2025).

Key Provisions and User Rights:

The Act establishes several critical rights for data principals. Users possess the right to provide informed, revocable consent prior to any processing of their personal data. Beyond consent, the Act empowers individuals with the right to access their data held by organizations, a right to rectification (correction) of inaccurate information, and a right

to erasure (deletion) of data under specified circumstances (Government of India, 2023). These rights are designed to provide meaningful control over personal information and to enable users to course-correct their digital footprints. The Act also establishes a right to grievance redressal, with mechanisms for users to lodge complaints and seek remedies for violations.

Importantly, privacy notices and consent forms are legally required to be drafted in clear, accessible language with a strong preference for presentation in regional Indian languages to promote broader inclusion and comprehension among India's highly multilingual population (PRS Legislative Research, 2025). This provision directly reflects the Act's commitment to substantive privacy rights and serves as a response to empirical evidence revealing widespread user confusion and disengagement when confronted with legalistic or linguistically inaccessible consent requests. The legislative intent is clear: rights are meaningful only when users can understand and exercise them.

Enforcement and Accountability:

The Data Protection Board, established as the regulatory and enforcement authority, wields substantial powers. The Board is empowered to levy significant financial penalties—reaching up to ₹50 crore per violation—to organizations that fail to comply with the Act's provisions (Government of India, 2023). This graduated penalty structure aims to create meaningful deterrence while acknowledging variations in organizational scale and intent. The Board is also tasked with issuing guidance, investigating complaints, and ensuring that both public and private sector entities adhere to data protection standards.

The Act distinguishes between regular data fiduciaries and "Significant Data Fiduciaries" (SDFs), based on the scale of data processing and potential societal impact. SDFs face enhanced obligations, including the requirement to appoint specialized Data Protection Officers (DPOs), conduct regular data protection audits, implement privacy-by-design principles, and maintain robust breach notification procedures (PRS Legislative Research, 2025). This tiered governance approach acknowledges that large-scale processors of personal data pose greater risks and therefore warrant stronger accountability mechanisms.

Collectively, these provisions represent an ambitious attempt to shift privacy from being an aspirational value to a lived, enforceable right—premised on the ideal of privacy as a shared, participatory responsibility between individuals and institutions. Yet, as subsequent sections of this study will demonstrate, statutory rights alone are insufficient without parallel focus on the everyday user practices and technical-institutional realities that shape data protection on the ground (EY India, 2024; PwC India, 2024).

Conceptual Framework: Security as Practice and Self-Directed Protection

This research is anchored in a conceptual framework that moves beyond purely legal or technological analysis to examine privacy as an integrated socio-technical practice. The approach draws from critical scholarship in security studies, organizational behavior, and human-computer interaction to understand how privacy protections actually function—or fail to function—in everyday life (Schneier, 2000; Williams, 2020).

Security as Process, Not Product:

Bruce Schneier's (2000) foundational observation that "security is a process, not a product" remains profoundly relevant to contemporary discussions of data protection. Security extends beyond legal provisions or technological products; it is a dynamic, ongoing practice requiring continuous attention, technical tools, legal literacy, and informed habits embedded within supportive governance structures. This perspective challenges the common misunderstanding that statutory enactment of a privacy law automatically translates into privacy protection. Instead, it insists that genuine privacy is realized through the sustained interaction of technical, behavioral, institutional, and cultural factors.

The Dual-Lens Framework:

This study utilizes a dual-lens conceptual framework encompassing:

Technical Practices: The technical lens encompasses digital tools and infrastructures such as encryption protocols, multi-factor authentication systems, password managers, virtual private networks (VPNs), breach notification systems, and privacy dashboards (Cherckesova et al., 2024; TeamPassword, 2023). These elements establish the baseline for secure data management and compliance, providing the technological infrastructure upon which privacy protection depends. However, technical tools remain limited in their protective efficacy if end-users lack the skills, literacy, or motivation to utilize them effectively. Moreover, poorly designed security interfaces can paradoxically reduce protection by encouraging users to disable safeguards or resort to risky workarounds (Cherckesova et al., 2024).

Non-Technical Practices: The non-technical dimension foregrounds the sociocultural and behavioral factors that drive or inhibit privacy protection. Key foci include the structure and accessibility of privacy governance, levels of digital privacy literacy, inclusiveness in design, institutional transparency, and trust-building between users and data fiduciaries (Bennett et al., 2020; Friedman et al., 2022). Importantly, this lens highlights how systemic barriers—such as linguistic complexity, interface design choices, socioeconomic inequalities, and digital infrastructure gaps—can prevent users from exercising their privacy rights meaningfully, even when strong legal protections are formally in place (AlZain et al., 2022).

Self-Directed Data Protection:

The overarching concept of "self-directed data protection" emerges as critical to the framework. It emphasizes the agency and active participation of individuals in safeguarding their own privacy—engaging thoughtfully with privacy notices, adopting technical safeguards appropriate to their risk profile, seeking institutional support or redress when necessary, and developing informed habits around data sharing (Westin, 2023; Williams, 2020). Without this active participation and empowerment, legal and technical measures risk becoming underutilized or ineffective, particularly among digitally marginalized populations.
This dual-lens approach acknowledges that privacy is both an individual and collective undertaking, demanding both accessible, usable technology and a supportive governance ecosystem. It places at the center of analysis the "user experience gap"—the persistent mismatch between what privacy laws promise and what users actually experience in practice (Renaud & Kelley, 2021). This gap persists due to a combination of legal complexity, technical usability challenges, uneven digital literacy, organizational capacity constraints, and insufficient attention to inclusion.

Literature Review

Digital privacy legislation cannot be fully understood without situating it within the broader discourse on privacy governance, socio-technical complexities, and user agency. This section synthesizes key findings from global and Indian scholarship to establish the evidence base for this study's focus on user experience as a critical dimension of privacy protection.

Global Best Practices and Persistent Challenges:

Internationally, leading privacy frameworks such as the European Union's General Data Protection Regulation (GDPR) emphasize the need to balance strong technical safeguards with user-centered design to foster transparency, institutional accountability, and effective individual empowerment (European Union, 2018). However, numerous empirical studies demonstrate that the persistence of legal complexity and poor interface designs significantly impair users' ability to engage meaningfully with privacy mechanisms. AlZain et al. (2022) found that legalese-filled privacy notifications substantially reduce user comprehension and meaningful engagement with privacy choices. Bennett et al. (2020) similarly document how trust in institutions, transparency of organizational practices, and perceived control all critically influence whether individuals adopt privacy-protective behaviors.

Emerging scholarship also highlights how cognitive biases condition privacy behavior. Renaud and Kelley (2021) demonstrate that optimism bias—the tendency to underestimate personal vulnerability to data breaches—significantly reduces motivation to adopt protective habits. These findings underscore that privacy protection is not merely a matter of providing information or technical tools; rather, it depends on psychological, social, and institutional factors that shape how individuals perceive risks and opportunities.

Compliance Maturity and Sectoral Variation in India:

In India's context, organizational readiness for DPDP compliance varies considerably across sectors. Research by EY India (2024) reveals that regulated sectors such as finance and telecommunications demonstrate relatively more developed privacy protections and compliance understanding, while small and medium enterprises (SMEs) and emerging digital service providers significantly lag behind. This sectoral disparity reflects differences in resources, regulatory history, and organizational capacity rather than uniform commitment to privacy principles.

PRS Legislative Research (2025) highlights that awareness gaps coupled with organizational constraints create cascading effects: organizations struggle to implement user-centered consent mechanisms, which in turn leaves users confused and disengaged. This feedback loop perpetuates the user experience gap. The challenge is particularly acute because SMEs, which constitute the majority of India's digital economy, lack the resources and expertise to redesign privacy processes, often defaulting to generic legal templates that fulfill minimal compliance requirements but do not prioritize user experience or accessibility (PwC India, 2024).

Digital Literacy and Inclusive Access:

A critical theme emerging across literature is the role of digital literacy and linguistic accessibility in determining whether statutory privacy rights are meaningful. Cherckesova et al. (2024) document persistent usability challenges with privacy-enhancing technologies: stronger security controls can become harder to use, inadvertently nudging users toward risky behaviors such as password reuse, disabling authentication features, or abandoning services altogether. This tension between security strength and usability highlights the critical importance of user-centered design in privacy implementation (Friedman et al., 2022).

In India's multilingual and socioeconomically stratified context, language accessibility takes on heightened importance. Privacy notices presented exclusively in English effectively marginalize large segments of the population, undermining principles of equitable access embedded in the DPDP Act (PRS Legislative Research, 2025). This linguistic gap exacerbates existing inequalities in digital literacy and access, creating a form of digital exclusion that disproportionately affects vulnerable populations including non-English speakers, older adults, rural users, and economically disadvantaged groups.

Emerging Institutional Responses:
On a positive note, the DPDP Act's enactment has catalyzed institutional innovations. Organizations increasingly establish dedicated Data Protection Officer (DPO) roles and privacy teams, signaling growing organizational commitment to privacy as a core governance function (EY India, 2024). Growing consumer awareness about data risks and privacy values presents opportunities for behavioral change. Additionally, emerging technological tools—such as consent managers, privacy dashboards, and user-friendly audit mechanisms—offer promising avenues to reduce the experience gap between legal intent and user practice (IBM Security, 2024).

Research Gap Addressed by This Study:
While substantial literature exists on privacy law, technical safeguards, and organizational compliance, fewer studies examine the integrated user experience landscape in non-Western contexts with significant digital inequality. This study addresses this gap by centering user experiences within India's digital privacy governance ecosystem, using empirical data to identify actionable pathways for translating formal rights into lived protections.

Research Question and Rationale

Central Research Question:
How does India's DPDP Act (2023–2025) expose both practical challenges in user comprehension—particularly regarding terms and consent—and promising avenues for embedding user-centered data privacy within digital governance?

Research Rationale:
This central inquiry is motivated by three interconnected concerns. First, the DPDP Act was enacted against a backdrop of limited public awareness and understanding of digital privacy risks among Indian users (PwC India, 2024). Preliminary evidence suggests that many individuals continue to experience digital privacy as an elusive ideal rather than a concrete reality they can exercise and benefit from. Second, the Act prioritizes user empowerment through informed consent mechanisms, yet consent is only meaningful if it is accessible, understandable, and actionable (AlZain et al., 2022). Third, the Act's success ultimately depends on translating formal legal protections into practices that users can meaningfully adopt, which in turn requires understanding the specific barriers users face (Westin, 2023).

The research foregrounds several sub-questions that guide the investigation:
·What is the current level of user awareness regarding DPDP provisions, rights, and mechanisms?
·What barriers do users encounter in understanding and acting upon their privacy rights?
·How do user experiences with consent mechanisms differ across demographic groups, regions, and linguistic backgrounds?
·What design and implementation changes would enhance users' ability and motivation to exercise their privacy rights?
·How can policy interventions bridge the gap between legal intent and user practice?

Methodology

Research Design and Approach:
This study employs a mixed-methods approach that triangulates primary empirical data with secondary sources and policy analysis. The integration of quantitative survey findings with qualitative policy analysis enables a comprehensive understanding of both broad patterns and specific contextual complexities shaping privacy practice in India (Saifi, 2025).

Primary Data Collection: Survey Design and Implementation:
An anonymous online survey was conducted in 2025, targeting urban, digitally engaged youth and professionals aged 18–55 from Delhi and Tamil Nadu. This purposive sampling strategy focused on individuals likely to interact routinely with digital platforms governed by the DPDP Act, ensuring relevance to the study's focus on user experiences. The sample comprised 52 respondents, which, while not statistically representative of India's entire population, provides rich qualitative and quantitative insights into user experiences among digitally engaged segments—segments critical to understanding DPDP implementation challenges.

Survey Instrument:
The survey instrument was developed through a systematic process involving review of the DPDP Act's text, consultation with privacy scholars and practitioners, and pilot testing with an initial respondent cohort. The instrument included multiple question types designed to assess:

·Awareness and familiarity: Questions assessing respondents' knowledge of DPDP provisions, rights conferred, and institutional mechanisms (e.g., Data Protection Board, complaint procedures)
·User experiences with consent: Questions exploring respondents' encounters with privacy consent forms, ease or difficulty of understanding terms, and behaviors when confronted with complex language
·Privacy tool adoption: Questions about usage of technical safeguards including password managers, two-factor authentication, VPNs, and privacy settings adjustments
·Identified barriers: Open and closed-ended questions probing obstacles users experience, including linguistic, usability, institutional, and literacy-related barriers
·Design preferences: Questions eliciting user preferences for how privacy information should be presented, including language, format (visual aids, plain language, multilingual support), and interface design features
Pilot testing with 8 respondents refined question clarity, identified potential confusion points, and improved survey flow. The finalized instrument balanced quantitative closed-ended items (enabling frequency analysis and pattern identification) with open-ended qualitative items (enabling respondents to articulate specific experiences and preferences in their own words).

Secondary Data Sources:
To contextualize and validate primary findings, the study draws extensively on secondary sources including:
·Policy reports and regulatory analyses from PwC India (2024), EY India (2023, 2024), and PRS Legislative Research (2025)
·Academic publications examining privacy behavior, digital literacy, and governance in India and comparative contexts (AlZain et al., 2022; Bennett et al., 2020; Renaud & Kelley, 2021)
·Government documents including the DPDP Act text, Rules 2025, and statements from the Ministry of Electronics and Information Technology (Government of India, 2023)
·Industry surveys on DPDP awareness and organizational compliance preparedness
·International comparative materials including GDPR implementation literature and global privacy framework analyses (European Union, 2018)
This mixed secondary source approach ensures triangulation across different perspectives—industry, civil society, academic, and governmental—and enables validation of primary survey findings against documented trends in organizational compliance and policy implementation.

Data Analysis:
Quantitative survey responses were analyzed using descriptive statistics (frequencies, percentages, central tendency measures) to identify patterns in awareness, tool adoption, and barriers. Responses were disaggregated by demographic characteristics (age, gender, language preference, education level) to identify variations across

subgroups and potential digital divide dimensions. Qualitative open-ended responses were subjected to thematic content analysis, with coding focused on identifying recurring themes, user sentiments, and specific pain points in consent experiences. Through this mixed-methods approach, both the breadth of user experiences and the depth of specific contextual factors shaping privacy practice become visible (Saifi, 2025).

Ethical Considerations:
This study adheres to strict ethical standards to protect respondents' rights and data confidentiality. All participation was voluntary, with informed digital consent obtained before survey commencement. The survey was designed to collect no personally identifiable information (PII); respondents remained anonymous throughout data collection and analysis. Data were stored securely with access restricted to the researcher. No individual responses are identifiable in any publications or reports emerging from this research. This ethical framework was designed to maximize respondent candor while protecting their privacy and upholding research integrity standards.

Study Limitations:
The study acknowledges several important limitations that shape interpretation of findings. The research sample was urban-based, relatively tech-savvy, and concentrated in two regions (Delhi and Tamil Nadu), likely overstating awareness and digital literacy levels compared to rural, older, and non-English speaking populations who face greater vulnerability to digital exclusion. The sample size, while providing rich qualitative insights, is not statistically representative of India's 1.4+ billion population. Additionally, the survey captures a single temporal snapshot (2025) and cannot track longitudinal changes in behavior or policy impact over time. These limitations suggest that future research should expand geographical reach, include more diverse demographic segments, and employ longitudinal designs.

Findings

Finding 1: Significant Awareness Deficit
The survey results reveal a striking lack of awareness and familiarity with the DPDP Act among urban, digitally engaged users. Only 22% of respondents reported being very familiar with the Act, presenting a concerning baseline given that this cohort represents a more digitally literate segment of India's population (Saifi, 2025). Approximately 44% stated they were not at all familiar with the DPDP Act, while 34% felt only somewhat familiar. This distribution indicates that a large majority lacks comprehensive knowledge of their statutory privacy rights—a troubling finding that directly challenges the Act's transformative potential.
More concerning than the mere statistic is the source of information through which respondents became aware of privacy issues. Rather than learning through official government campaigns, institutional communications, or credible educational outreach, the primary sources were informal channels including social media platforms and word-of-mouth (Saifi, 2025). This pattern suggests that official awareness campaigns have been insufficient to reach even tech-savvy populations, indicating need for substantial public education infrastructure development.

Finding 2: Partial but Confused Engagement with Privacy Practices
The survey reveals moderate engagement with privacy protection behaviors alongside significant usability challenges. A majority (68%) reported actively using privacy settings or withdrawing consent at least once from digital applications or services. Furthermore, 55% reported utilizing privacy-enhancing tools such as strong passwords, two-factor authentication, and VPNs (Saifi, 2025). These figures suggest that users possess some awareness of privacy risks and have adopted protective behaviors.

However, this aggregate engagement masks substantial frustration with implementation. Notably, 75% of respondents who had made concerted efforts to adjust privacy controls described these procedures as confusing, time-consuming, or inefficient (Saifi, 2025). This disconnect—between the existence of protective behaviors and the user experience of those behaviors as burdensome—reveals the user experience gap at the heart of this study. Users are adopting protective measures but doing so despite, rather than because of, usable design and clear guidance. These findings align with global research documenting the usability challenges of privacy-enhancing technologies (Cherckesova et al., 2024).

Finding 3: Consent Complexity as Barrier to Meaningful Choice

A prominent and consistent finding concerned widespread user difficulties in understanding and meaningfully interacting with terms of service, privacy notices, and consent forms. Open-ended responses revealed recurrent themes of confusion and disengagement (Saifi, 2025). Representative quotes included "I don't understand website consent—so I leave the site," "Legal language makes it hard for me to know what I'm agreeing to," and "The privacy terms are so long, I just click accept to get on with it." This pattern of disengagement reflects a fundamental breakdown in the consent mechanism envisioned by the DPDP Act (Government of India, 2023).

Critically, when respondents attempted to exercise their rights—such as withdrawing consent—they encountered significant obstacles. Very few participants could confidently articulate the procedure to withdraw consent once given, or could explain specifically what rights they possessed under the DPDP Act (Saifi, 2025). This ignorance directly results in digital exclusion: rather than making an informed choice about service engagement, users frequently abandon applications or platforms entirely, losing access to services that could benefit them. The intended protective mechanism of informed consent thus becomes a barrier to digital access. These patterns corroborate findings by AlZain et al. (2022) and Bennett et al. (2020) regarding the detrimental impact of legal complexity on user comprehension and engagement.

Finding 4: Multilayered Barriers to Privacy Exercise

Respondents identified multiple, intersecting barriers to understanding and acting on their privacy rights (Saifi, 2025). These barriers cluster into several categories:

·Linguistic barriers: Insufficient availability of privacy information in regional Indian languages. Users whose first language is not English reported substantially greater difficulty understanding consent mechanisms, even when fluent in English for everyday communication.

·Usability barriers: Interface design choices that obscure privacy options, make withdrawal difficult, or present information in hard-to-navigate formats. Users expressed frustration with having to locate privacy settings across multiple menus or interfaces.

·Institutional trust barriers: Mistrust stemming from vague or overloaded privacy notices that fail to clearly explain data uses. Users reported skepticism about whether organizations would truly honor privacy preferences.

·Literacy and digital skills barriers: Lack of foundational understanding about what personal data comprises, what risks data misuse poses, or what concrete steps provide protection. This barrier disproportionately affects older adults and individuals with lower educational attainment.

·Systemic exclusion: Structural digital exclusion affecting populations with limited internet access, older devices, or poor connectivity, preventing participation in digital services and the privacy protections they theoretically provide.

These findings align with research demonstrating how cognitive, linguistic, and structural barriers compound to limit privacy agency (Friedman et al., 2022; Renaud & Kelley, 2021).

Finding 5: User-Articulated Preferences for Improvement

Despite these barriers, respondents articulated clear, actionable preferences for how privacy communications could be improved (Saifi, 2025). The largest demand was for privacy tools and notices conveyed in simple, plain language in users' own languages, recognizing and responding to India's linguistic plurality. Respondents consistently requested that "Decline" and "Withdraw consent" options be made as prominent and easy as "Accept" choices, addressing current manipulation patterns in interface design. Visual aids—including step-by-step guides, infographics, and visual consent management dashboards—were widely cited as helpful features that could enhance clarity and reduce cognitive burden. Respondents also emphasized desire for contextual, just-in-time education about privacy risks and available protections.

Finding 6: Organizational Capacity and Compliance Variation

Beyond user-level findings, respondents and secondary sources revealed substantial organizational readiness gaps. Large organizations with dedicated privacy teams demonstrated greater capacity to implement user-centered privacy practices, though even large firms often defaulted to generic legal templates (EY India, 2024). SMEs, which constitute the majority of India's digital economy, reported substantial difficulties due to lack of budgeted resources, absence of privacy expertise, or awareness of design alternatives. Secondary sources (EY India, 2024; PwC India, 2024) corroborated this finding, documenting that compliance gaps are particularly pronounced among smaller organizations, which may inadvertently marginalize their users through poorly designed consent mechanisms. Additionally, the survey revealed low awareness of the penalties imposed under the DPDP Act and limited publicized enforcement actions, reducing deterrence and organizational incentive for compliance improvements (Saifi, 2025). The gap between the Act's penalty structure and public awareness of enforcement thus undermines the intended deterrent effect.

Discussion

The empirical findings corroborate and extend global patterns documented in privacy scholarship while revealing India-specific complexities (AlZain et al., 2022; Bennett et al., 2020). This section synthesizes findings within broader analytical frameworks to illuminate paths forward.

The Usability Crisis:

The first major finding—that large majorities of respondents who attempt privacy actions describe the experience as confusing, time-consuming, or burdensome—reveals what might be termed a "usability crisis" in current privacy implementations (Saifi, 2025). This crisis undermines the DPDP Act's foundational commitment to user empowerment (Government of India, 2023). When individuals attempting to exercise their rights encounter barriers, they rationally respond by disengaging rather than persisting. The consequence is paradoxical: legal rights theoretically protect citizens, yet the poor usability of rights-exercise mechanisms results in those rights remaining unarticulated and unexercised.

Research by AlZain et al. (2022) and Bennett et al. (2020) documented similar phenomena globally. However, India's context compounds these challenges. The linguistic diversity of India means that a privacy notice in English alone excludes large populations from meaningful engagement (PRS Legislative Research, 2025). The digital literacy variation across regions and socioeconomic strata further stratifies who can effectively navigate complex consent interfaces. This observation leads to a critical realization: the digital divide is not only about access to technology, but also about access to meaningful understanding of rights and ability to exercise them through usable interfaces (Friedman et al., 2022).

Institutional Capacity as Implementation Bottleneck:

The second major finding—organizational readiness gaps, particularly acute among SMEs—reveals that legal enactment alone is insufficient to drive behavioral change (EY India, 2024; PwC India, 2024). The DPDP Act places substantial obligations on organizations to implement privacy-by-design, deploy appropriate technical safeguards, and ensure consent mechanisms are truly meaningful (Government of India, 2023). Yet many organizations, particularly resource-constrained SMEs, lack the capacity, knowledge, or financial resources to translate these mandates into practice.

This capacity gap creates several problematic dynamics. First, SMEs may resort to compliance theater—appearing to comply with legal requirements through minimal-effort generic templates rather than genuinely implementing privacy-centered practices. Second, the gap creates a competitive disadvantage, where organizations committed to genuine privacy protection face higher costs than competitors cutting corners. Third, the gap perpetuates the user experience problem: organizations lacking capacity are least likely to invest in user-centered design that could mitigate usability barriers (PwC India, 2024).

The Digital Inclusion Imperative:

A third major theme emerging from the findings is that privacy protection, when poorly implemented, becomes a vector of digital exclusion rather than empowerment. Users confronted with incomprehensible consent terms or complex privacy controls respond rationally by withdrawing from digital services entirely (Saifi, 2025). For vulnerable populations—including non-English speakers, older adults, rural users, and economically disadvantaged groups—this withdrawal can represent a substantial loss of opportunity. If banking, government services, healthcare, and educational platforms require navigating confusing privacy terms to access services, then those unable to navigate this complexity are excluded from essential services.

This observation points to a critical justice implication of privacy governance: privacy implementation choices have distributive consequences. Poorly designed privacy mechanisms do not harm all users equally; they disproportionately exclude those with fewer educational, linguistic, or technical resources (Friedman et al., 2022). Conversely, privacy frameworks that prioritize inclusion—through multilingual support, visual design, simplified language, and accessible interfaces—can become vehicles for more equitable digital participation.

Positive Trends and Institutional Evolution:

Despite the challenges documented above, the findings also identify positive developments suggesting that DPDP implementation, while nascent, has catalyzed important institutional changes. Organizations increasingly establish dedicated Data Protection Officer roles and privacy teams, signaling that privacy governance is becoming a recognized organizational function (EY India, 2024). Growing consumer awareness about data risks, though still inadequate, represents a foundation upon which education campaigns can build. Technological innovations—including consent managers, privacy dashboards, and simplified audit mechanisms—are being deployed by leading organizations and offer replicable models for broader adoption (IBM Security, 2024).

Critical Analysis: The Gap Between Law and Practice

These findings collectively reveal what might be characterized as a "governance implementation gap"—the distance between what statutory law prescribes and what organizations actually implement, what users actually experience, and what protections actually materialize in practice (Westin, 2023). This gap is not unique to India; it characterizes privacy regulation across diverse contexts (European Union, 2018). However, India's particular context—with its linguistic diversity, digital infrastructure inequality, and significant variations in organizational capacity and digital literacy—intensifies the implementation challenge (PRS Legislative Research, 2025).

Importantly, this gap is not inevitable. Other jurisdictions demonstrate that it can be substantially reduced through deliberate policy choices, investments in education, regulation of design practices, and support for organizational capacity building. The existence of the gap in India is thus not a reflection of inherent limitations but rather a reflection of current policy priorities and resource allocations.

Policy Recommendations and Implementation Pathways

Based on the research findings, this section proposes priority recommendations organized by stakeholder group to bridge the gap between the DPDP Act's aspirational vision and everyday user reality.

Recommendations to Government and Regulatory Bodies

1. Establish Privacy Interface Design Standards: The Data Protection Board should develop evidence-informed minimum standards for privacy notice design—including font sizes, language complexity, color contrast, and multilingual requirements (Friedman et al., 2022). Enforcement should include regular compliance audits with corrective action requirements for violations.
2. Mandate Digital Privacy Literacy Programs: The government should fund comprehensive digital privacy education initiatives delivered through schools, community centers, and public media in all major Indian languages (PRS Legislative Research, 2025). Programs should progress from basic awareness (what is personal data, why it matters) to actionable skills (managing privacy settings, filing complaints).
3. Support Organizational Capacity Building: Establish SME support programs providing access to privacy compliance toolkits, design templates, and subsidized audits (PwC India, 2024). Incentive structures—such as public recognition or reduced regulatory scrutiny—can encourage genuine privacy practices over compliance theater.

Recommendations to Organizations and Data Fiduciaries

1. Redesign Privacy Notices for Clarity: Organizations should simplify privacy notices to a grade-6 reading level using visual hierarchies, infographics, and layered information structures (AlZain et al., 2022). Critically, notices must be available in users' preferred languages with equal visibility for "Decline" and "Withdraw" options to eliminate dark patterns (Friedman et al., 2022).
2. Implement User-Friendly Consent Management: Deploy transparent consent dashboards enabling users to easily view collected data, withdraw specific consent categories, and understand data purposes (IBM Security, 2024). These tools should feature plain-language explanations and visual risk indicators.
3. Provide Just-in-Time Privacy Education: Rather than front-loading information at signup, deliver contextual privacy guidance when users make data-sharing decisions (Williams, 2020). For example, explain location data implications when users enable location tracking.

Recommendations to Civil Society and Research Institutions

1. Develop Open-Source Compliance Toolkits: Create publicly available, freely licensed templates and design guidelines that SMEs and public bodies can adapt. Lower barriers to adoption among resource-constrained organizations.
2. Conduct Independent Privacy Audits: Civil society research organizations should regularly audit how major digital platforms implement privacy notices, consent mechanisms, and data handling. Publish findings in accessible formats to create public accountability pressure.
3. Establish Measurement Frameworks: Develop empirical models and assessment frameworks evaluating whether consent mechanisms enable genuine informed choice and whether privacy implementations reduce or exacerbate digital inequality (Saifi, 2025). These measures should be scientifically rigorous and actionable for continuous improvement.

Case Study: The Banking Application Experience

To illustrate these themes concretely and ground them in human experience, consider the following case study examining an individual's encounter with digital privacy challenges under the DPDP framework.
The Experience:
A 22-year-old undergraduate student in Delhi, whom we will call Maya, decided to register for a digital banking application to manage her finances independently. Upon opening the application, she encountered a lengthy consent form presented exclusively in English. The form contained multiple sections with dense legal terminology: discussions of "data controllers," "processing categories," "legitimate interests," "third-party recipients," and "consent withdrawal procedures." The language was technically precise but impenetrable to someone without legal training (Saifi, 2025).

Maya attempted to understand what she was consenting to. The form did not explain in accessible language what data would be collected, why the bank needed it, with whom it would be shared, or what risks it faced. No visual aids, infographics, or simplified summaries guided her understanding. After spending fifteen minutes reviewing the form without achieving meaningful comprehension, Maya faced a difficult choice: agree to terms she did not understand or abandon the process and forgo the digital banking service that would facilitate her financial independence.
Feeling uncertain and uncomfortable consenting to something she did not understand, Maya abandoned the registration process. She retained her reliance on a physical bank branch and avoided the digital banking service—a choice reflecting protective caution but also resulting in digital exclusion from essential financial services.
Analysis:

This case study illuminates several dimensions of the privacy governance challenge relevant to the DPDP Act's implementation:
1. Usability as Justice: The experience illustrates how consent mechanisms that fail to communicate effectively become not tools for user empowerment but barriers to digital access (AlZain et al., 2022). The legal right to informed consent means little if the information provided is not actually informative. This represents a justice failure: individuals theoretically possess rights to privacy and control, yet interface design choices prevent meaningful exercise of those rights. Particularly for young people beginning to engage with digital financial services, such barriers can establish lasting patterns of digital exclusion.
2. Linguistic Accessibility and Inclusion: Maya's experience as an English speaker—yet finding English-language legal terminology inaccessible—points to the greater challenges faced by speakers of other Indian languages (PRS Legislative Research, 2025). For someone whose first language is Tamil, Hindi, Kannada, or another regional language, the English-only consent form would be even more impenetrable. This raises fundamental questions about equity: does access to the digital economy depend on English fluency? Current consent practices suggest an implicit answer of "yes," which discriminates against India's non-English-speaking majority and reflects failure to implement the DPDP Act's mandate for local-language privacy information (Government of India, 2023).
3. The Organizational Perspective: From the bank's standpoint, the consent form represented compliance with legal requirements: it covered all necessary information, included appropriate legal protections, and obtained written acknowledgment. The organization was technically compliant with legal requirements yet failed the deeper purpose of privacy law: enabling users to understand and control how their data is used (Westin, 2023). This disconnect points to a systemic problem: compliance-focused approaches optimize for legal risk reduction rather than user understanding, inadvertently undermining the law's protective purpose.

4. Policy Implementation Lessons: This case illustrates that the DPDP Act's vision of user empowerment through informed consent cannot be realized through legal mandate alone (Government of India, 2023). It requires parallel investments in design excellence, organizational culture change, and user education. Without these complementary investments, the statutory right to informed consent remains theoretical.
5. Digital Inclusion Imperative: Perhaps most importantly, this case illustrates how privacy implementation choices have distributive consequences (Friedman et al., 2022). When consent mechanisms are poorly designed, all users experience friction; however, users with greater educational attainment, English fluency, and confidence in navigating unfamiliar digital interfaces can more easily overcome this friction. Users lacking these characteristics face greater barriers and are more likely to abandon services. Over time, this divergence creates digital inequality: technology that theoretically serves everyone in practice serves those with particular educational and linguistic characteristics.

Limitations and Future Directions

While this study provides valuable insights into user experiences with India's DPDP Act and identifies pathways toward improved implementation, several limitations merit acknowledgment:

Sample Limitations: The research sample was urban-concentrated, relatively tech-savvy, and limited to two regions (Delhi and Tamil Nadu), likely overstating awareness and digital literacy levels compared to rural populations, older adults, and non-English speakers who face greatest vulnerability to digital exclusion (Saifi, 2025). The sample size, while enabling rich qualitative insight, is not statistically representative of India's diverse population. Findings should therefore be understood as providing indicative patterns among digitally engaged urban segments rather than representative of India writ large.
Temporal Limitation: This study captures a single temporal snapshot in 2025, the initial implementation phase of the DPDP Act. Privacy governance landscapes evolve as regulations mature, organizational practices change, and user understanding develops. Longitudinal research tracking implementation over time would provide more robust understanding of how these factors evolve.
Sectoral and Geographic Limitation: The study concentrates on general user experiences but does not deeply examine sector-specific variations (financial services, healthcare, government platforms) or geographic variations between urban and rural contexts. Future research should explore how privacy challenges and opportunities differ across sectors and regions.

Future Research Directions:
Several avenues for future research emerge from this study's limitations:
1. Expanded Geographic and Demographic Scope: Future studies should extend research to rural regions, include older adults, non-English speakers, and individuals with lower educational attainment to understand how privacy implementation affects diverse populations and contributes to digital inequality.
2. Longitudinal Implementation Studies: Multi-year research tracking DPDP implementation would enable understanding of how organizational practices, user awareness, and actual privacy outcomes evolve over time and how policy interventions affect these trajectories.
3. Pilot Program Evaluation: Experimental or quasi-experimental studies should evaluate the efficacy of specific interventions—such as visual consent managers, simplified privacy notices, or community literacy programs—in improving user understanding and participation.

4. Sectoral Deep-Dives: Future research should examine how privacy challenges and opportunities vary across sectors (finance, healthcare, government, social media, e-commerce) and develop sector-specific guidance for implementation.
5. International Comparative Research: Comparative analysis of how other Global South countries implement privacy frameworks, their successes and challenges, and lessons applicable to India would enrich understanding of governance possibilities.

Conclusion

India's Digital Personal Data Protection Act provides an ethical and rights-based blueprint for digital citizenship in an increasingly data-driven world (Government of India, 2023). The Act's legislative ambitions—establishing clear data principal rights, fiduciary duties, institutional enforcement mechanisms, and mandates for plain-language communication—represent genuine policy innovation and demonstrate governmental commitment to digital privacy protection. However, this study demonstrates that the Act's transformative potential depends fundamentally on bridging the critical divide between formal legal protections and the lived experiences of users in all their diversity (Saifi, 2025).

The research reveals that informed consent, positioned as a cornerstone of digital privacy protection, is only meaningful if it is accessible, understandable, and actionable for diverse user populations across India's multilingual and socioeconomically stratified landscape (AlZain et al., 2022; Bennett et al., 2020). Current implementations frequently fail this test, rendering consent mechanisms counterproductive through their complexity, linguistic inaccessibility, and poor usability. Simultaneously, the study documents that organizational readiness gaps, particularly acute among SMEs, prevent many organizations from translating legal mandates into user-centered practices (EY India, 2024; PwC India, 2024). These interconnected challenges produce what this research terms the "user experience gap"—the distance between what privacy law promises and what users actually experience in practice.

The findings carry several critical implications for policy and practice. First, privacy protection is not primarily a matter of having strong laws; it is a matter of translating laws into usable, understandable practices that people can meaningfully engage with (Schneier, 2000; Williams, 2020). Second, privacy implementation has distributive consequences: poorly designed privacy mechanisms disproportionately exclude those with fewer linguistic, educational, and technical resources, potentially exacerbating rather than alleviating digital inequality (Friedman et al., 2022). Third, effective privacy governance requires coordinated action across government (enforcement, capacity building, awareness), organizations (design excellence, user support), and civil society (advocacy, research, community education).

Looking forward, digital privacy governance must evolve into a practice that integrates three elements: technological tools that are both robust and usable; institutional accountability structures that are independent and transparent; and active user participation supported through education and inclusive design (Westin, 2023). Policymakers, organizations, civil society, and research institutions must collaboratively advance inclusive privacy frameworks that support self-directed data protection as a routine social practice rather than a regulatory checkbox—a challenging aspiration, but one essential to fulfilling the DPDP Act's promise.

By fostering such an integrative approach, India can not only fulfill its legislative commitments under the DPDP Act but also serve as a global exemplar for equitable, participatory, and resilient digital rights governance in complex sociotechnical contexts. The stakes are high: privacy protection in the digital age fundamentally shapes who can participate in digital services, who benefits from digital opportunities, and whose interests are protected in an increasingly data-driven society. The DPDP Act provides the legal foundation; translating that foundation into lived protection for all remains the essential challenge ahead.

References

AlZain, M., Soh, B., & Pardede, E. (2022). Digital privacy awareness and literacy gaps among internet users: A systematic review. Computers & Security, 118, 102738. https://doi.org/10.1016/j.cose.2022.102738
Bennett, C. J., Parsons, C., & Molnar, A. (2020). Trust and sociological factors in data protection: Evidence from privacy behaviour research. Policy & Internet, 12(3), 345–367. https://doi.org/10.1002/poi3.225
Cherckesova, L., Safaryan, O., Revunkov, G., & Ivanov, D. (2024). Development of password manager using cryptographic algorithms and VPN integration. International Journal of Advanced Computer Science and Applications, 15(2), 234–251. https://doi.org/10.14569/IJACSA.2024.0150234
European Union. (2018). General Data Protection Regulation (Regulation 2016/679). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
EY India. (2023, August 22). Decoding the Digital Personal Data Protection Act, 2023: Implications for Indian businesses. https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023
EY India. (2024, June 24). EY survey reveals organizational readiness for DPDP Act implementation: Challenges and opportunities. https://www.ey.com/en_in/newsroom/2024/06/ey-survey-reveals-organizational-readiness-for-dpdp-act-implementation
Friedman, B., Hendry, D. G., & Borning, A. (2022). Design and accessibility in data security: A value sensitive design approach. MIT Press.
Government of India. (2023). Digital Personal Data Protection Act, 2023. Ministry of Electronics and Information Technology.
https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%2C2023.pdf
IBM Security. (2024). Data privacy examples: AI and IoT security risks in the digital age.
https://www.ibm.com/security/artificial-intelligence
PRS Legislative Research. (2025). Digital Personal Data Protection Bill, 2023: Analysis and implementation challenges. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023
PwC India. (2024, October 21). Survey on DPDP awareness and organizational preparedness: Key findings from consumer and business perspectives. https://www.pwc.in/press-releases/2024/only-16-consumers-in-india-understand-the-digital-personal-data-protection-dpdp-act.html
Renaud, K., & Kelley, T. (2021). Optimism bias in security behavior: The role of perceived control and risk assessment. Journal of Cybersecurity, 7(3), 1–14. https://doi.org/10.1093/cybsec/tyab015
Saifi, A. (2025). Security-as-practice: User experiences with India's DPDP Act [Unpublished survey data]. Department of Political Science, Jamia Millia Islamia.
https://docs.google.com/forms/d/1pLCh4cKLNc_RnV65VIiFBMLWB_8hihFm5UIZVS9E6AQ/edit#responses
Schneier, B. (2000, April). The process of security. Information Security, 3(4), 12–17.
https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html
TeamPassword. (2023, March 15). Password manager and VPN integration: Enhanced security for distributed teams. https://teampassword.com/blog/password-manager-and-vpn
Westin, A. F. (2023). Privacy law developments: From theory to practice in digital governance. Journal of Information Policy, 13(2), 54–72. https://doi.org/10.5325/jinfopoli.13.2023.0054
Williams, K. R. (2020). Security orchestration and incident response: Building resilient digital ecosystems. Cybersecurity Review, 52, 24–39. https://doi.org/10.1089/cyber.2020.5024