INCIDENTAL EXPOSURE IN THE DIGITAL COMMONS: CROWD-SOURCED CARTOGRAPHY, UNINFORMED PHOTO CONTRIBUTION, AND THE UNRESOLVED PRIVACY CRISIS ON GOOGLE MAPS IN INDIA: A LEGAL COMMENTARY

Mukti Jain, Alliance University

ABSTRACT

India hosts one of the world's largest and fastest-growing populations of internet users. Yet explosive connectivity has not been matched by an equally explosive growth in digital literacy. This commentary examines a phenomenon that sits at the intersection of platform design, user ignorance, and regulatory inadequacy: the accidental public exposure of private residences and intimate family imagery through crowd-sourced contributions to Google Maps. Drawing on India's constitutional right to informational privacy, the Information Technology Act, 2000 ("IT Act"), the Digital Personal Data Protection Act, 2023 ("DPDP Act"), and comparative jurisprudence, it is argued that the current legal framework fails to adequately address this mode of incidental exposure. Three regulatory failures are identified: the absence of a proactive duty on platforms to distinguish residential from commercial listings; the structural inadequacy of the intermediary safe harbour under Section 79 of the IT Act as applied to photo-contribution features; and the incomplete operationalisation of the DPDP Act. The commentary concludes with recommendations directed at Parliament, the Data Protection Board of India, and the platforms themselves.

I. Introduction: Connectivity Without Comprehension

India today has over 800 million internet users,[1] a figure that is projected to continue rising as smartphone penetration deepens in semi-urban and rural geographies. The Digital India programme has made internet access structurally cheaper than at any prior point in the country's history.[2] This democratisation of connectivity is rightly celebrated. Yet access to the internet and comprehension of its consequences are not coextensive. A user who pays fifty rupees per month for a data plan is not thereby equipped to understand that uploading a family photograph to a review platform may render it permanently and globally public, geotagged to their home, and visible to over a million strangers.

This commentary is concerned with a specific, underanalysed instance of that comprehension gap. Google Maps - the dominant mapping service in India - operates a crowd-sourced contribution system through which registered users, known as "Local Guides," may submit photographs, reviews, and locational data about places. The system is designed to improve the richness of the platform's information. In practice, however, it generates two privacy risks that have attracted almost no sustained legal analysis in the Indian context.

The first risk is locational: private residential premises are frequently listed as public or semi-public locations on Google Maps, often as a by-product of delivery addresses being crowd-sourced or suggested by the platform's own algorithms. The second risk is photographic: users, frequently without appreciating the public character of their uploads, post intimate personal and family imagery - including imagery that, absent contextual knowledge, may be profoundly misread by third-party viewers - in connection with these publicly listed residential pins. The aggregate effect is that the private home is digitally dissolved into the public sphere.

This commentary proceeds as follows. Part II describes the mechanics of the exposure phenomenon. Part III analyses the constitutional foundations of the right to privacy as they bear on this issue. Part IV examines the statutory framework, focusing on the IT Act and the DPDP Act. Part V constructs a hypothetical but legally realistic case study. Part VI identifies the structural deficits of the current framework. Part VII offers specific recommendations.

[1]Telecom Regulatory Authority of India (TRAI), Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector (2018).
[2]Internet and Mobile Association of India (IAMAI) & Nielsen, India Internet 2023 Report (2023) <https://www.iamai.in> accessed 12 April 2026.

II. The Mechanics of Crowd-Sourced Exposure

A. How Residences Become Public Listings

Google Maps populates its database through a combination of satellite imagery, licensed geospatial data, and user contributions.[3] The Local Guides programme - Google's gamified contribution platform - incentivises ordinary users to submit information about locations in exchange for points, badges, and other non-monetary rewards.[4] While the programme is primarily oriented toward commercial establishments, nothing in its design confines it to them. A user may suggest, edit, or confirm any location - including a private residence - as a named, reviewable, publicly accessible point on the map.

The risk is compounded by the rise of hyperlocal delivery infrastructure. Delivery personnel - who, as a demographic, are among the most active contributors of location data to mapping platforms - frequently pin private homes as named landmarks to simplify future navigation. Once pinned, a residence may accumulate reviews from other delivery personnel, photographs of the facade or gate, and a permanent public identity on the platform's interface. The homeowner is given no notification. No consent is sought. No mechanism for objection is built into the contribution flow.

B. The Photo Contribution Problem

The photograph contribution feature of Google Maps presents a distinct but related privacy risk. When a user attaches a photograph to a location pin, that image is uploaded to Google's servers, associated with that geolocation, and made publicly visible to every user who views the relevant listing. The uploader typically does not appreciate the permanence of this action, the impossibility of controlling downstream distribution once an image is indexed, or the fact that their upload immediately acquires public character.

The volume that such contributions can reach is striking. A single prolific contributor may upload thousands of photographs, accumulating millions of collective views - views that, critically, are driven not by any directed decision of the contributor but by the platform's

[3]Frontiers in Computer Science, "Awareness of Privacy and Data Collection: Exploring Privacy Policy Effectiveness in Google Maps" (2025) 7 Frontiers Comput Sci <https://doi.org/10.3389/fcomp.2025.1568179> accessed 12 April 2026.

[4]Google, "Google Maps Contributions Policy" (Google, 2024) <https://maps.google.com/intl/en_in/help/maps/hereandnow/> accessed 12 April 2026.

algorithmic surfacing of content. The contributor uploads; the algorithm amplifies; the result is exposure at a scale wholly disproportionate to the contributor's intent or awareness.

A particular risk arises from photographs of family gatherings, cultural festivals, or private ceremonies posted in association with residential pins. Absent contextual knowledge - knowledge that only the participants possess - such photographs may be grossly misread. Imagery of traditional play, ritual, or ceremony may carry implications of harm or danger to a viewer entirely unfamiliar with the cultural context. This creates not only reputational risk but the potential for intervention by third parties - including, in extreme cases, law enforcement - based on a wholly distorted reading of benign family activity.

The platform's own Acceptable Use Policy prohibits the distribution of personal information without consent.[5] However, this prohibition is framed primarily as an obligation on downstream users of the Maps API, not as a substantive safeguard governing the contribution flow itself. The gap between policy text and platform design is precisely where the privacy harm resides.

III. Constitutional Foundations: Informational Privacy and the Puttaswamy Framework

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[6] a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution of India. The judgment is significant for present purposes in at least three respects.

First, Justice Chandrachud, writing for the plurality, situated privacy not merely as a negative right - the right to be free from interference - but as a positive right to control the narrative of one's own life: "privacy includes within itself the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation."[7] This formulation is directly relevant to the present issue, since the home and family life are precisely the domains violated by unconsented residential listing and family imagery upload.

Second, Justice Kaul's concurring opinion articulated the dimension of informational

[5]Google, "Google Maps Platform Acceptable Use Policy" (Google Cloud, 2025) <https://cloud.google.com/maps-platform/terms/aup/help-center> accessed 12 April 2026.
[6]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[7]ibid [180] (Chandrachud J).

privacy with particular clarity, recognising the right to protect personal data and to control information about oneself.[8] His Lordship stressed that data protection and the right to be forgotten must form part of India's constitutional privacy architecture - a demand that has since been partially (and still incompletely) answered by the DPDP Act.

Third, the Court's observation that "the collection of information about a person gives power over them"[9] anticipates precisely the asymmetry created by crowd-sourced cartography: a private individual's residence, movements, and intimate family life are converted into public data without their knowledge, creating power that may be exploited by strangers for purposes ranging from commercial targeting to physical harm.

Critically, however, *Puttaswamy* concerned primarily the vertical relationship between citizen and State. The horizontal application of privacy rights against private actors - including technology corporations - remains insufficiently theorised in Indian jurisprudence. The constitutional right articulated in *Puttaswamy* thus requires statutory translation to be effectively enforceable against platforms such as Google. The IT Act and the DPDP Act are the primary instruments of that translation, and it is to these that the analysis now turns.

IV. The Statutory Framework and Its Deficits

A. The Information Technology Act, 2000: The Intermediary Safe Harbour

Section 79 of the IT Act provides the foundational framework governing intermediary liability in India. Under Section 79(1), an intermediary - defined broadly to include search engines, mapping services, and platforms hosting user-generated content[10] - is not liable for third-party information, data, or communication links hosted by it.[11] This conditional immunity is the structural mechanism by which platforms like Google Maps escape liability for user-uploaded content in ordinary course.

The immunity is not absolute. Section 79(3)(b) provides that an intermediary loses its protection where, upon receiving "actual knowledge," it fails to expeditiously remove or

[8] ibid [523] (Kaul J).
[9] ibid [308] (Chandrachud J).
[10] Information Technology Act 2000 (India), s 2(w).
[11] Information Technology Act 2000 (India), s 79(1).

disable access to unlawful material.[12] The Supreme Court in *Shreya Singhal v. Union of India* read down this provision to require, at minimum, a court or government order before the "actual knowledge" threshold is triggered.[13] The Intermediary Guidelines of 2021 further require platforms to appoint grievance officers and to maintain a "notice and take-down" mechanism.[14]

In the context of residential listings and photo contributions, this framework produces a troubling result. A homeowner who discovers that their home has been listed as a public location on Google Maps - or that family photographs have been uploaded without their knowledge - must first identify the relevant content, then submit a complaint to the platform's grievance officer, then await a response, and then, if unsatisfied, seek a court order compelling removal. This is an onerous burden for most individuals and an effectively impossible one for those in semi-urban or rural areas without legal sophistication or resources. More fundamentally, the framework is reactive: it addresses harms only after they have materialised and been drawn to the platform's attention, by which point the content may have been viewed by millions.

B. The Digital Personal Data Protection Act, 2023

The DPDP Act, enacted in August 2023 and partially operationalised by the DPDP Rules 2025 notified in November 2025, represents India's first comprehensive statutory framework for digital data protection.[15] Its core architecture imposes obligations on "data fiduciaries" - entities that determine the purpose and means of processing personal data - to obtain free, informed, specific, and unambiguous consent before processing, and to process data only for the specified purpose.[16][17]

The Act's application to the scenario under discussion is, however, complicated by a critical exclusion: it does not apply to personal data "made publicly available by the Data Principal herself."[18] This exclusion, designed to avoid over-regulation of voluntarily shared

[12]Information Technology Act 2000 (India), s 79(3)(b).
[13]Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India), [118]–[119] (Nariman J), interpreting "actual knowledge" under s 79(3)(b) IT Act as requiring a court or government order.
[14]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India), r 3(1)(b).
[15]Digital Personal Data Protection Act 2023 (India) (No 22 of 2023), s 2(j) (defining "data fiduciary"), s 2(n) (defining "digital personal data").
[16]Digital Personal Data Protection Act 2023 (India), s 4(1).
[17]Digital Personal Data Protection Act 2023 (India), s 6(1).
[18]Digital Personal Data Protection Act 2023 (India), s 3 (scope), read with the proviso excluding data "made

information, creates a structural gap in the exact situation this commentary addresses. Where a third party - not the data principal but a family member, a delivery worker, or a passing contributor - uploads photographs or location data, the "public availability" exception may not apply. Yet the Act's enforcement regime, which is being implemented in phases through May 2027,[19] remains insufficiently precise on the question of whether platforms that passively host such contributions qualify as data fiduciaries with respect to those specific data points.[20]

The DPDP Rules 2025 impose a notice-before-processing requirement and a purpose limitation principle that, on their face, should govern photo contributions in relation to identifiable individuals.[21] The difficulty is that the practical enforcement gap - between the statutory text and the reality of millions of uninformed users uploading content to a global platform - has not yet been addressed through regulatory guidance, adjudication, or platform-specific rulemaking.

V. A Constructed Case Study

Consider the following illustrative scenario. A family resides in a semi-urban neighbourhood in a northern Indian city. Over several years, their home address has been pinned on Google Maps as a named location, initially because delivery services found it useful. A family member - educated, professionally employed, and socially active - regularly contributes photographs to Google Maps as part of the Local Guides programme. Over time, they upload nearly two thousand photographs across various locations. Many of these photographs are taken at home during festivals and family occasions and are uploaded to the residential pin, which appears on the platform as a public location.

Among the uploads are photographs of a family's Holi celebration. That year, due to a bereavement in the family, the traditional use of coloured water and powder had been replaced by play with dry sand. Photographs of the occasion - taken in good faith and uploaded without appreciation of their public character - depict multiple family members buried to their necks in sand. Without contextual knowledge of the tradition being observed and the modification made

publicly available by the Data Principal herself".

[19]Hogan Lovells, "India's Digital Personal Data Protection Act 2023 Brought into Force" (Hogan Lovells, November 2025) <https://www.hoganlovells.com> accessed 12 April 2026.

[20]Digital Personal Data Protection Rules 2025 (India), r 3 (notice requirements); Ministry of Electronics and Information Technology (MeitY), notification dated 13 November 2025.

[21]Puttaswamy (n 6) [308] (Chandrachud J): "the collection of information about a person gives power over them" - recognising informational self-determination as a core dimension of privacy.

that year, the photographs present a scene that a reasonable third-party viewer might interpret as depicting a violent or threatening act. The images have, by the time any family member becomes aware of the issue, received over 2.7 million views across the platform.

This scenario illustrates the multi-layered nature of the harm. There is a locational harm - the private residence has become a public listing. There is a photographic harm - intimate family imagery has been exposed at massive scale. There is a contextual integrity harm, in the sense described by Helen Nissenbaum: information (a family ritual) appropriate in one context (private celebration) has been transmitted to a wholly different context (public global platform) in a manner that distorts its meaning. And there is a safety harm - the family's home address, combined with imagery suggesting potential violence, creates a risk profile for the household that did not previously exist.

The uploader in this scenario is not malicious. They are a well-educated adult acting in what they understood to be a social and communal spirit. The harm is precisely the product of the gap between digital access and digital literacy - a gap that the law, as presently constituted, does not require platforms to bridge.

VI. Structural Deficits: Three Failures of the Current Framework

A. The Absence of a Proactive Duty to Distinguish Residential Listings

Neither the IT Act nor the DPDP Act imposes any affirmative obligation on mapping platforms to distinguish, algorithmically or procedurally, between commercial and residential pins, or to require consent before a residential address is confirmed as a named public location. This is a categorical failure. The legal literature on informational privacy - both in India and comparably regulated jurisdictions - recognises that the home carries a heightened privacy expectation.[22] Comparative regulatory practice in the European Union under the GDPR and the United Kingdom's ICO guidance on street-level imagery has begun to impose heightened

[22]Aaron Boring & Christine Boring v. Google Inc., 598 F.Supp.2d 695 (WD Pa 2009); Hiroshi Kato, "Google Street View and the Law: The Japanese Approach to Blurring and the Right to Privacy" (2010) 19(2) Pac Rim L & Pol'y J 435.

obligations in relation to residential data.[23] [24] [25] India has no equivalent instrument.

B. The Safe Harbour as a Shield Against Victims

Section 79's safe harbour was designed to foster the growth of online intermediaries by insulating them from liability for content they did not generate. In the context of photo contributions, however, the provision operates as a structural disincentive to proactive platform design. Because Google Maps faces no liability unless it receives "actual knowledge" (via court or government order) of unlawful content, it has no legal incentive to redesign the contribution flow to include consent prompts, residency warnings, or contextual misinterpretation alerts. The burden of remediation falls entirely on the victim, who must navigate a complex and time-consuming complaint process while the content continues to be viewed.

This structural design reflects a policy choice that may have been appropriate in the early period of internet platform development but which is poorly calibrated to an environment in which a single platform hosts billions of user-generated contributions and an individual uploader's content may reach millions of viewers within weeks. The Intermediary Guidelines of 2021 have moved incrementally in the direction of greater platform accountability through grievance officer requirements and additional due diligence obligations,[26] but they do not specifically address the design defects of photo contribution features.

C. The Digital Literacy Lacuna

The deeper structural failure is cultural and educational rather than strictly legal: the law cannot be effective as a privacy protection mechanism if users do not understand the legal consequences of their digital actions.[27] India's digital literacy initiatives, such as those under the Digital India programme,[28] have focused primarily on enabling access and transactional

[23]Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) [2016] OJ L 119/1, art 17 (right to erasure), art 22 (automated individual decision-making).
[24]UK Information Commissioner's Office, "Guidance on Street-Level Imagery" (ICO, 2022) <https://ico.org.uk> accessed 12 April 2026.
[25]Telecom Regulatory Authority of India (TRAI), Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector (2017) 14–15.
[26]Niti Aayog, National Strategy for Artificial Intelligence (Government of India, 2018) 45 (identifying digital literacy as a prerequisite for equitable AI and data governance).
[27]Usha Ramanathan, "A Unique Identity Bill" (2010) 45(35) Economic & Political Weekly 10, 11 (observing that Indian data governance historically presumed technical sophistication among subjects of data collection).
[28]IT Rules 2021 (n 14), r 4(2) (requiring significant social media intermediaries to appoint a Grievance Officer accessible to Indian users).

use. They have not meaningfully addressed privacy consciousness - the understanding that digital action creates public and permanent data trails with legal implications for oneself and for others whose data one uploads. Niti Aayog's National Strategy for Artificial Intelligence identified digital literacy as a prerequisite for responsible data governance,[29] but this identification has not translated into literacy programming specifically oriented toward privacy.

A significant feature of this failure is its cross-socioeconomic character: the problem is not confined to those with limited education or income. Educated, professionally employed, and digitally active users are equally capable of uploading thousands of photographs to a public platform without understanding the legal implications of doing so. This undermines any regulatory approach that relies on user awareness as a substitute for platform-level safeguards.[30]

VII. Recommendations

A. For Parliament and the Data Protection Board of India

The Data Protection Board of India ("DPBI"), whose establishment was notified in November 2025, should issue binding regulatory guidance clarifying that crowd-sourced geolocation data attached to identifiable residential premises constitutes "digital personal data" within the meaning of the DPDP Act, and that platforms hosting such data in association with user-uploaded photographs act as data fiduciaries in respect of those data sets. This guidance should specify that the public availability exception does not apply where the data was made publicly available by a third party rather than the data principal.

Parliament should further consider amending Schedule I of the DPDP Act or the DPDP Rules 2025 to include residential location data as a category of sensitive personal data, mandating explicit consent before such data is listed, confirmed, or rendered searchable on mapping platforms. The penalty framework under Section 17 of the Act should be applied to platforms that fail to implement consent-based residential data flows after a reasonable

[29]Press Information Bureau, Ministry of Electronics and Information Technology, "Digital India" (Government of India, 2023) <https://www.digitalindia.gov.in> accessed 12 April 2026.
[30]Digital Personal Data Protection Act 2023 (India), s 17 (penalties ranging from INR 10,000 to INR 250 crore for data breaches and non-compliance).

compliance period.

B. For Platforms

Google, as the dominant provider of mapping services in India, should be required - whether by regulatory direction or voluntary commitment - to implement the following design changes. First, a consent-verification step before any residential address is confirmed as a named public listing, distinguishing such listings from commercial establishments. Second, a contextual warning presented to users who upload photographs in association with a residential pin, informing them of the permanent, public, and globally accessible character of their upload. Third, a simplified takedown mechanism for data principals who wish to remove photographs or residential listings associated with their homes, operable without legal representation and resolved within a prescribed period.

C. For Digital Literacy Programmes

The Ministry of Electronics and Information Technology and state-level implementation agencies should design and deploy digital literacy curricula that specifically address informational privacy - the understanding that uploading a photograph creates a permanent, public, and legally consequential data trail. These curricula should be targeted not only at first-time internet users but at existing, experienced users who have not received any formal instruction in privacy consequences. The lesson of this commentary is that formal education and professional employment are not proxies for privacy literacy. A programme that reaches only the digitally naive will not address the structural problem.

VIII. Conclusion

The privacy crisis examined in this commentary is quiet, pervasive, and largely invisible to the law. It does not announce itself in the form of a data breach or a hacking incident. It accumulates, incrementally, through the ordinary contributions of ordinary users who believe - reasonably, on the basis of their experience - that they are doing something local and personal when they upload a photograph or confirm an address on a mapping platform. The result, in aggregate, is the dissolution of the private home into the public digital commons, achieved without consent, without notice, and without any adequate legal remedy.

The constitutional framework established by *Puttaswamy* provides a strong doctrinal

foundation for the protection of informational privacy as a fundamental right. The statutory framework of the DPDP Act provides the legislative skeleton of a protection regime. What is missing is regulatory specificity, platform-level accountability, and a genuine cultural investment in privacy literacy commensurate with the scale of India's digital expansion. Until those three elements are in place, the gap between cheap internet and responsible digital citizenship will continue to impose real and underappreciated harms on families across India who have done nothing more than share their life online.