

Response to the Department of Post's DHRUVA Policy Document

Dvara Research is an independent, non-partisan, not-for-profit policy research institution based in India. Its mission is to ensure that every low-income household and every small enterprise has complete access to suitable financial services and social security. Over the past few years, we have thought carefully about the ideal design of digital public infrastructure (DPI) to support government service delivery to citizens. Our previous work on the same is [available here](#).

In this document, we present our response to the policy document on [DHRUVA \(Digital Hub for Reference and Unique Virtual Address\): The Digital Address DPI](#), hereafter referred to as the '*policy document*', published by the Department of Posts in May 2025.

The policy document sets out the vision for a DPI for address management in India. It establishes the need for a DPI approach to address management, based on concerns that the current addressing system is fragmented and relies on narrative conventions, causing disrupted and inefficient service delivery across public and private sectors. A set of potential use-cases from the perspectives of citizens, governance administrators, and the private sector are discussed. The document also lays out an envisioned institutional and legal framework for the DPI.

We divide our recommendations in two sections. Section A offers recommendations for the design and functionality of the DHRUVA database. Section B provides recommendations on the institutional design and the supporting legal framework.

A. Recommendations on the design and functionality of the DHRUVA database:

1. It is unclear if the proposed design of the database is suited to geospatial governance.

We welcome the objective of using geospatial data for better city-planning, strengthening climate resilience and overall governance. One of the primary motivations for the construction of DHRUVA is “enabling geospatial governance to enable informed decision-making on key governance priorities such as welfare distribution, citizen safety, and economic efficiency, including optimal resource allocation” (p.16). This approach is also in line with leading international efforts on strengthening the availability of geospatial, interoperable information systems such as the United Nation’s Integrated Geospatial Information Framework ([IGIF](#)). These intended uses of the digital address database have the potential to be impactful, transformative tools of governance. However, it is unclear if the database is designed to enable decision making for administrators at the collective-level.

It appears that the design of the database upholds decentralization, through its federated design, data-blindness, and user-controlled data sharing through consent-based data sharing mechanisms. It is unclear how this would permit for data aggregation which is a pre-requisite for decision-making at the collective-level. For instance, when determining the location of a new school or hospital in a city, the planner would need to understand the number of people in the area, the way they are spread in the region etc. However, from the current design it is unclear how such data, which may be located across different AIPs may be aggregated, how relevant population would be identified given the system’s

data-blindness and subsequently, how consent from each person would be obtained and ultimately, how the accuracy of the decision would be affected if consent were denied. These safeguards cannot be dismantled for the sensitive nature of the data, but it may be worth assessing the utility of personal information in an address information management system. It appears that not only does the presence of personal information attract more obligations, but it may also reduce the utility of the database for collective-level decision making.

Collective-level decision making is a compelling reason for the creation of such databases. The Australian database Geocoded-National Address File (G-NAF)¹ for instance has been instrumental in modelling bushfires and bolster readiness in tackling them. The US' National Address Database (NAD) also supports transport planning, disaster management and emergency response, school zoning, etc.² Similarly, Europe's INSPIRE Knowledge base seeks to harness address data (among other things) for the purpose of environmental policy and research and coordinating emergency responses.³

The absence of personal information in these datasets permits hosting the dataset openly (like in Australia). Such datasets also do not attract user-consent requirements because they do not contain any personally identifiable information. Such address management systems that comprise addressable data only (containing no reference to personally identifiable information), appear better suited to solve policy problems at the regional, state, or national levels, which is often a pressing objective for the creation of these databases in the first place. The necessity for a federated structure, consent and data blindness arise from the personal and sensitive information being collected by the system. A database devoid of personal information would create fewer obligations and potentially offer better tools for collective, policy-level decision making.

Recommendations: We request a detailed consideration of how the DHRUVA database may facilitate collective-level decisions.

2. The DHRUVA system introduces risks of exclusion (from welfare service delivery) arising from the transition to a digital addressing system.

Welfare distribution appears to be a core application for the DHRUVA system (p. 7, p.14, p.17, p.24). An important policy learning in the aftermath of the COVID pandemic pertained to the mobility of India's large migrant population and their families. The One Nation, One Ration Card (ONORC) system intended to relieve such individuals of the burden of proving their domicile address in a given state and hence allowed beneficiaries to collect their Public Distribution System (PDS) benefits in any part of the country, no matter the place of residence.⁴ Similarly, the provision of welfare in the form

¹ Barclay, S. (n.d.). Rethinking Bushfire Resilience: Leveraging BAL Ratings to Foster Safer, More Sustainable Communities. Accessed from: <https://geoscape.com.au/impact-stories/rethinking-bushfire-resilience/>

² US Department of Transportation. (2025). National Address Database. Accessed from: [National Address Database | US Department of Transportation](#)

³ European Commission. (n.d.). INSPIRE: Infrastructure for Spatial Information in Europe. Accessed from [INSPIRE Knowledge base - European Commission](#)

⁴ Ministry of Consumer Affairs, Food and Public Distribution. (2021). "Implementation of ONORC Scheme". Accessed from: [Implementation of ONORC scheme](#)

of Direct Benefit Transfers (DBTs) into bank accounts has made the need for address data less important than in the past. Reverting to an address-centric design of welfare distribution could recreate the causes of exclusion that have been remedied over the past few years.

Further, it is also unclear whether the DHRUVA address database is designed for the purpose of welfare distribution. Though not mentioned explicitly in the document, it appears residence (*and not ownership*) is the grounds for generating a Digital Postal Index Number (DIGIPIN). A person could link their name to an address by the simple virtue of living in it and not necessarily owning it. Therefore, there may be a divergence between the domicile address which is often the basis for receiving welfare support and the place of residence. This may exacerbate exclusion, as opposed to easing it. For instance, the system envisions support for ‘audit trails for benefit disbursement’ (p. 26), allowing administrators visibility over where and when benefits were delivered. Such a system might flag (say) a benefit trail reflecting collection across different addresses as fraudulent; whereas, such a benefit trail may also represent beneficiaries whose locations change frequently. To suspend disbursement of benefits to such beneficiaries based on the system’s capability to track addresses would be erroneous.

Further, the policy document does not clearly set out the technological abilities, minimum standards of equipment etc.⁵ that might be needed for users to engage with Address Information Agents (AIAs.) Experience with implementing large-scale digitisation projects in India indicate that a) those at the socio-economic margins struggle the most to adapt to such systems, and b) existing modes of intermediations are replaced by others, which may bring new and unique risks to the beneficiary⁶.

Recommendation: We recommend that the use of DHRUVA for social protection be limited to geospatial governance at the collective-level, rather than for personalised and targeted service delivery.

3. DHRUVA system may benefit from a wider suite of channels to collect addresses.

The system proposes collecting address data exclusively from the individual end-user (citizen), who may create/update/deactivate their digital addresses with AIAs. AIAs in turn register the DIGIPIN-digital address combination with Address Information Providers (AIPs). Thus, the responsibility for collation of address data into the DHRUVA ecosystem is not initiated by the state or administrator but rests on each individual citizens’ participation in the system.

It is unclear, for instance, what happens if some citizens do not generate DIGIPINS and digital addresses against their residences, implying that some addressable locations may be left out of the dataset altogether. The policy document does not specify how completeness of the database may be ensured. It is also unclear how the system would handle situations wherein (say) two individuals may generate digital addresses against the same parcel of land, or how the system would resolve multiple addresses that may occur at the same parcel of land (such as a multi-storeyed apartment building). The

⁵ IIT Hyderabad. (2025). IIT Hyderabad, Department of Posts, and NRSC (ISRO) Collaborate to Launch DIGIPIN: A National-Scale Geospatial Addressing System for India. Accessed from <https://pr.iith.ac.in/pressrelease/IITHDIGIPIN.pdf>

⁶ Dvara Research. (2023). State of Exclusion: Delivery of Government-to-citizen cash transfers in India. Accessed from dvararesearch.com/wp-content/uploads/2024/01/State-of-Exclusion-Delivery-of-Government-to-Citizen-Cash-Transfers-in-India.pdf

ability of the system to deliver on its promises rests in its ability to collect accurate, up-to date, and near ubiquitous address information.

The system proposes Address Verification Agencies (AVAs) and Confidence Scores to gauge the accuracy of the information. However, in the absence of details, it is unclear how those may be applied at population scale given the diversity and physical expanse of the country. Currently, there are also no measures to ensure that the information will be updated at stipulated frequencies which risks the dataset becoming outdated and losing its utility.

Recommendation: The system may benefit from harvesting a suite of channels to collect address information such as in-person surveys, using current data available with different public and private institutions. Instituting protocols to periodically check data quality and accuracy will also be crucial to the functioning of the database.

B. Recommendation on the legal and institutional framework supporting the DHRUVA system

1. The collection of personally identifiable data including for the creation of a digital public infrastructure should be supported by a specific parliamentary legislation.

The policy document proposes a very intricate, complex system of entities and stakeholders such as the AIP, AIA, Address Information Users (AIU), Central Mapper, etc. It also provides an insight into processes such as user's consent, confidence scores, and a *Governance Entity* to support the functioning of the DHRUVA system.

A key factor differentiating the DHRUVA system from other geo-coded, geo-referenced national address databases appears to be its ability to link the personal identity of person, as well as the descriptive address and the geographical coordinates. Most national databases (such as in the USA, Australia, and France) do not link the personal identity of the person to the geo-coded, geo-referenced address.

The key role of the individual in the system, the collection of their personal information and the ability to link the individual to an address, together suggest that the DHRUVA database, even in its federated form rests upon the collection of highly sensitive personal information. In Puttaswamy I⁷ the Supreme Court explained that a law which affects individuals' privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them. Further,

⁷ Justice KS Puttaswamy (Retd.) and Another versus Union of India and Others, (Supreme Court of India August 24, 2017) <https://www.scobserver.in/wp-content/uploads/2021/10/Right to Privacy Puttaswamy Judgment 1.pdf>

Puttaswamy II⁸ judgement of the Supreme Court explained that a legislation backing any public scheme must have specific information such as the legitimate state aim which can be discerned from the aims, objectives, and introduction of the Act, for the Act to be considered valid. The legislation must also have provisions to ensure the security of the PII collected for the scheme. Finally, it has been reiterated in Puttaswamy I and Puttaswamy II that the legislation must also have provisions needed to test the necessity and proportionality of the scheme.⁹

The DHRUVA system would need a specific Act to support its creation. Though the Post Office Act, 2023 empowers “the central government to issue standards for the DIGIPIN and the Digital Address” (p. 33), the DHRUVA system is more nuanced than that. It contemplates a Governance Entity with the powers to oversee the functioning of the system including issuing and enforcing technical and conduct standards for the different stakeholders (AIA, AIU, AIP, AVA etc.). It also proposes the creation of confidence scores, validation mechanisms which may be built upon or produce further sensitive information. In summary, the DHRUVA system imagines collecting personal information, address information, the creation of an entity with rule making and supervisory powers, the creation of a new type of entity, the AIA. An Act that specifically allows for this intricate system may provide the adequate legal backing and provisions of the Post Office Act 2023 alone may be inadequate to provide the legal backing to these nuanced initiatives.

Recommendation: Supporting the DHRUVA framework through an enabling legislation by the Parliament that provides the aims, objectives, legality, necessity, proportionality and other provisions needed to pass the constitutional muster to create a digital address.

Table of abbreviations

Abbreviation	Full form
Digital Hub for Reference and Virtual Unique Addresses	DHRUVA
Digital Public Infrastructure	DPI
United Nation’s Integrated Geospatial Information Framework	IGIF
Geocoded-National Address File	G-NAF
National Address Database	NAD
One Nation, One Ration	ONOR
Public Distribution System	PDS
Direct Benefit Transfer	DBT

⁸ Justice KS Puttaswamy (Retd.) and Another versus Union of India and Others, (Supreme Court of India) Sept 26, 2018. Accessed from: https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf

⁹ Justice KS Puttaswamy (Retd.) and Another versus Union of India and Others, (Supreme Court of India September 26, 2018) https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf

Digital Postal Index Number	DIGIPIN
Address Information Agent	AIA
Address Information Provider	AIP
Address Verification Agency	AVA
Address Information User	AIU