# PLENARY WORKSHOP ON DIGITAL PUBLIC RECORDS

*Srijoni Sen and Trishi Jindal*

Workshop Report
August 2022

NATIONAL LAW SCHOOL
OF INDIA UNIVERSITY
BENGALURU

# ABSTRACT

The Digital Public Records Project at the National Law School of India University (NLSIU), Bangalore organised a Plenary Workshop on Digital Public Records on April 8-9, 2022. The Workshop aimed at assembling a select group of stakeholders across the bureaucracy, academia, civil society, and the developer community to exchange their perspectives and experiences, and inform research priorities under the project between April 2022-March 2023.

The project approaches the issue of government transparency in aid of securing the public's socio-economic and political rights through the lens of sound information management. As part of this, it seeks to undertake research on the extant public records management framework in India, alongside policy implications arising from limits to access and transparency imposed under laws focusing on privacy, security, and intellectual property. This report sheds light on the discussions that have shaped the research agenda and the researchers' narrowing of issues based on the discussions.

This project, including this report, is supported by the Thakur Foundation.

## CONTENTS

## BACKGROUND

Transparency of the government has come to be accepted as a common pro-democracy choice and ideal across polities. In India, the right to information (RTI) is seminal to accessing critical information regarding the working of the government. Most recently, the COVID-19 pandemic saw RTI queries revealing information regarding government spending on vaccines, recorded deaths, spending on PPE kits and the like, exemplifying the importance of transparency in assessing governance outcomes. At the same time, it is necessary to think about the very importance of such information – firstly, existing and second, being managed within public authorities. For instance, the World Health Organisation (WHO) recently released data on COVID-19 deaths in India. This has been controversially received as the Indian government has claimed the absence of such data, citing the failure of states to share deaths arising from oxygen shortages.[1] This is emblematic of an important issue vis-à-vis transparency, i.e., the criticality of sound information management within public authorities across governmental levels.

Before proceeding further, we would like to highlight how we understand some terms used repeatedly in this report. We understand 'public records' as per the wide definitions under the Right to Information Act, 2005 (RTI Act)and the Public Record Act, 1986 (PRA). Under these, 'public records' imply any record in any form which arises out of public authorities (which include government ministries, departments, authorities as well as corporations funded or controlled by the government), regardless of how they are made available to the public. We understand 'information' as that collection of data or records, which conveys meaning according to the context and the arrangement of such data, or records used. At the same time, it is necessary to distinguish between 'data' and 'record'. While definitions can vary, we understand a record (say a document) as a unit of evidence, while data comprises a unit of information, though both can overlap.

Keeping this in mind, another facet of government transparency is traced to open data movements. India has emphasised open data commitments, focusing on a new draft Data Use and Accessibility Policy 2022, revising its previous National Data Sharing and Accessibility Policy 2012 (NDSAP). However, we are scoping 'open government' through the lens of records management and access, where data management is a related but distinct concern.

On the digitisation front, the government has supplemented existing legal frameworks of the PRA and the RTI with disaggregated frameworks like the e-Pramaan framework for e-authentication for service delivery[2], an E-mail Policy for the government[3] and Best Practices & Guidelines for Production of Preservable e-Records (PRoPeR) 2014[4]. However, a cohesive understanding of records management, alongside ongoing revisions of privacy and security laws and policies within information laws remains hard to find.

[1] *No disaggregated data on Covid death, says Ministry of Health*, THE NEW INDIAN EXPRESS, February 9, 2022, available at https://www.newindianexpress.com/nation/2022/feb/09/no-disaggregated-data-on-covid-death-says-ministry-of-health-2417268.html.

[2] *e-Pramaan: Framework for e-Authentication (October 2012)*, available at https://epramaan.gov.in/publications.html.

[3] E-Mail Policy of the Government of India (October 2014), available at https://www.meity.gov.in/writereaddata/files/E-mail_policy_of_Government_of_India_3.pdf.

[4] Production of Preservable e-Records (PROPeR): Best Practices and Guidelines) (2013), available at http://www.ndpp.in/download/standard/Final_PROPeR_Best_Practices-01.pdf.

At this stage, therefore, it is important to invest research in how this digitisation is manifesting as an opportunity and a challenge towards streamlining records management in the absence of a cohesive understanding of the same. The Digital Public Records Project (DPR Project) at NLSIU, Bangalore is invested in researching how this streamlining of legal and policy frameworks can be undertaken for India.

Admittedly, the scope of the project is large, and the approach to the same can vary across (a) interests in transparency and accountability of public authorities, (b) improving effective public service delivery to secure socio-economic entitlement, (c) improving policymaking through participatory processes, etc. At this stage, we choose not to pick one over the other, and instead outline the following set of assumptions to ground our research questions under the project:

(a) The universe of information that qualifies as public records under existing statutes is vast. To this end, we need to first identify a clearer picture of its scope and criteria for categorising and organising public information.

(b) Management of public information is complex and fragmented, given the different stages of implementation and priorities of digitisation initiatives. Thus, governance challenges must necessarily involve a study of the implementation of digitisation and records management at the sectoral level to identify best practices and challenges that need addressing in a bottom-up law and policy framework.

(c) The freedom of information and the public interest in information entails both the duty to proactively disclose information and respond to distinct queries posed to public authorities. This freedom can be constrained through competing interests in national security, privacy and intellectual property and confidentiality protection. To ensure that these constraints operate without unreasonably quelling the public interest, sound information disclosure decisions need to be grounded in clearly articulated principles.

These assumptions led to us identifying three distinct sessions for the workshop to glean insights on each assertion, and identify narrower, more focussed research questions for the project.

The Keynote Speaker for the event was Dr Rajendra Kumar, Additional Secretary, MeitY, who also leads the e-governance group at the Ministry. His address identified the digitisation interests of the government, alongside an overview of current and past initiatives that ground e-governance and digitisation in India, to guide our discussions on the scope of digitisation of governance and the universe of digital public records in India.

The first session focused on whole-of-government perspectives on digitisation and public records management. The session was moderated by Ms Srijoni Sen, Visiting Assistant Professor, NLSIU and the Lead at the DPR Project. The panel comprised the following participants:

- Mr J Satyanarayana, former Chairman UIDAI and currently Chief Adviser, World Economic Forum
- Dr Sayeed Chaudhury, Johns Hopkins University, and former Member, National Museum and Library Services Board of the United States
- Dr Bidisha Chaudhuri, Associate Professor and M.Sc. (Digital Society) Programme Coordinator, IIIT Bangalore.

- Mr Anand Krishnan, Data Security Council of India.

The second session looked at records management as a systems challenge, gleaning perspectives on specific digitisation initiatives within the government, namely, land records digitisation and public finance records digitisation. The session featured a paper presentation by Ms Tarika Jain, Research Fellow at the Vidhi Centre for Legal Policy. The discussion thereafter was moderated by Trishi Jindal, Research Fellow at the DPR Project. The discussion featured the following speakers:

- Dr KP Krishnan, formerly Secretary, Economic Advisory Council to the Prime Minister.
- Mr Rajeev Chawla, formerly ACS Karnataka.
- Mr Deepak Sanan, Indian Institute for Human Settlements and Senior Visiting Fellow, Centre for Policy Research.
- Ms Tarika Jain, Vidhi Centre for Legal Policy
- Ms Sarah Farooqui and Ms Divya Chirayath, Centre for Budget and Government Accountability.

The third session focused on challenges associated with proactive disclosures and response to RTI queries under the RTI Act. The session was moderated by Ms Srijoni Sen, NLSIU and featured the following panellists:

- Mr Shailesh Gandhi, Former Central Information Commissioner, India
- Mr Venkatesh Nayak, Director-in-Charge, Commonwealth Human Rights Initiative
- Ms Amrita Johri, Satark Nagarik Sangathan
- Mr Gaurav Godhwani, CivicDataLab
- Dr Arul George Scaria, National Law University, Delhi

This paper carries a synthesis of the discussions that took place over the two days of the workshop, placed within analytical choices arrived at by the authors. While these are influenced and informed by the discussions under these three panels, they are not explicitly or implicitly endorsed or disputed by the panellists. The errors are the authors' alone. We extend our deepest gratitude to the panellists for their time and expertise.

## Overview of Issues

### I. Digitisation and Public Records

Digitisation of governance is taking place across different stages and governmental levels – e.g. under the MGNREGA scheme, (near) real time updating of muster rolls (workers' attendance sheets) is hosted online to monitor scheme implementation; Rajasthan state government collates scheme related information across departments on its online *Jan Soochna Portal*[5]; land records are being digitised under State and Central level programmes[6]; RTI filing has been digitised[7] to enable online RTI queries. Each of these initiatives have evolved over varied priorities and objectives: effective scheme monitoring, improving communication regarding public services to the public, clarifying title to land, enabling easier access and use of information across government departments and agencies, alongside improving information sharing among departments to improve policymaking.

Digitisation here entails conversion or creation of information – records, files, data – in a digital format, specifically moving away from the paper (or hard copy) versions. This research project recognises the centrality of information management – its creation and collection, storage, processing, preservation, destruction and dissemination – in ensuring accountable digital governments.

To this end, the project first aims to focus its thinking on the broader governance and sociological challenges associated with digitisation and information management. Through a discussion on digitisation experiences at the workshop, we received feedback from career bureaucrats, civil society leaders working on transparency of government, academics studying sociological impact of digital governance, and public policy leaders with experience of public records and archives from Indian and the American perspectives.

Specifically, the discussion highlighted three core issues to ground our research:

(a) The definition and scope of public records;
(b) The governance of public records; and
(c) The impact of digitisation on public records.

#### Definition and Scope of Public Records

#### ***Public records are records pertaining to public functions***

Foremost, it is important to acknowledge that public records are defined as such regardless of their public availability. Public records imply any record of a government agency or department or decision-making body. Notably, the understanding of public records is derived from the Indian Evidence Act, 1872, wherein any document forming acts or records of acts of public bodies in India, including public records of private documents are considered public documents.[8] In the context of the Public Records Act, 1993, any record in any form that emanates from a government

[5] *Jan Soochna Portal 2019*, available at https://jansoochna.rajasthan.gov.in/Home/HomePage.

[6] *Computerization of Land Records (CLR)*, Digital India Land Records Modernization Programme (DILRMP-MIS 2.0), available at https://dilrmp.gov.in/faces/percent/rptComputerizationOfLandRecord.xhtml/.

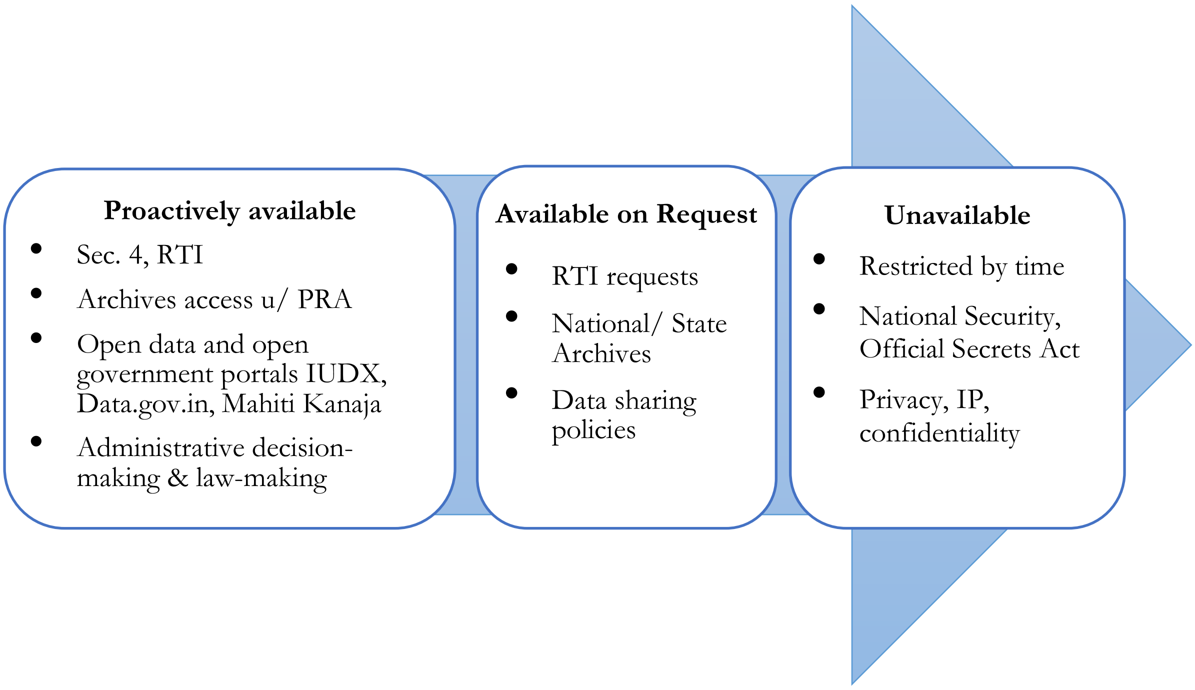
[7] *RTI Online*, available at https://rtionline.gov.in/.

[8] Section 74, Indian Evidence Act, 1872.

department, agency or undertaking is considered a public record,[9] and is thus covered under the protocol for preservation and destruction of the records provided under its framework for archiving of public records. The RTI Act similarly identifies any record of a public authority as covered under the regime for disclosure of public information under its framework.[10] The understanding of public records remains consistent throughout each of these - encompassing any record that pertains to a government body, agency or public authority, though there are some differences in the scope of public authorities covered.

They are thus considered eligible for preservation/ management/ destruction based on a prescribed protocol, as long as they are considered public records. One discussant also recommended approaching the definition and scope of public records from the point of view of *decisions* – wherein the decisions to act or not act, both are considered relevant for public information.

Given that public records are defined based on the fact they originate from a government department, agency or undertaking, their volume and scope is immense. In response, it was suggested that these vast volumes can be better managed through (a) clear timelines for retention tied to their classification as public, secret, confidential, etc. (b) considered engagement of external partners (discussed further in a section below), and (c) technical architecture that applies across the ecosystem with built-in protocols. Furthermore, citing the example of the US, one discussant pointed out that public records are defined under distinct categories earmarking the terms of retention, publishing and deletion of different types of records.



**Proactively available**

- Sec. 4, RTI
- Archives access u/ PRA
- Open data and open government portals IUDX, Data.gov.in, Mahiti Kanaja
- Administrative decision-making & law-making

**Available on Request**

- RTI requests
- National/ State Archives
- Data sharing policies

**Unavailable**

- Restricted by time
- National Security, Official Secrets Act
- Privacy, IP, confidentiality

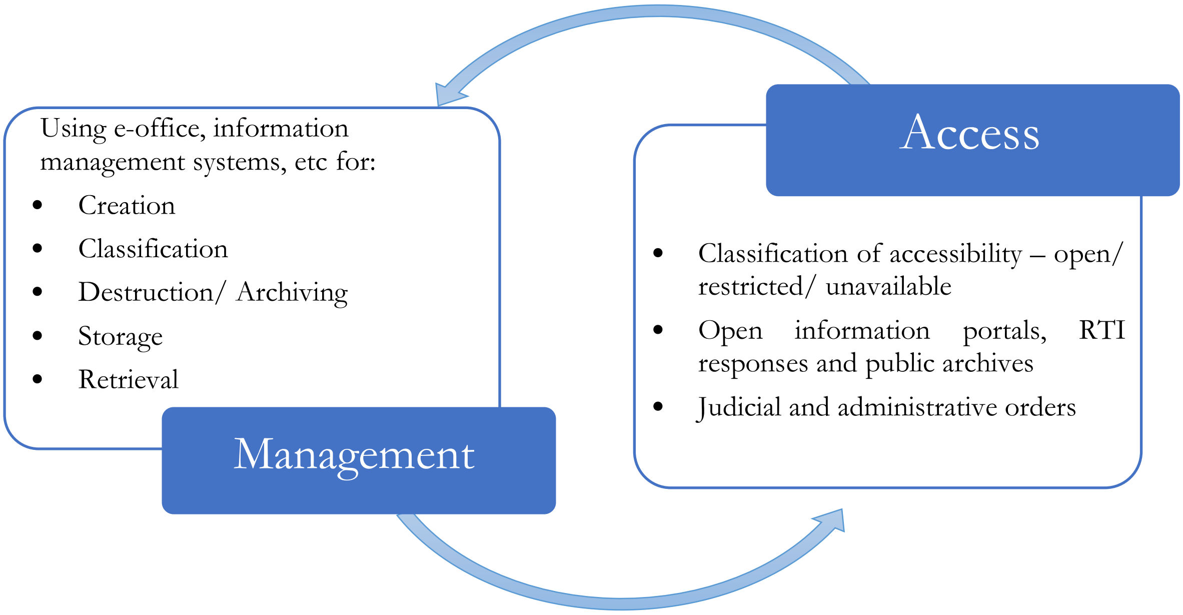
[9] Section 2(e) r/w 2(f), Public Records Act, 1993.

[10] Section 2(i), r/w Section 2(h), Right to Information Act, 2005.

### *Access and management of records are interlinked*

While their public availability is not a ground to define a public record, the manner of its preservation affects access. Under the RTI Act, Section 4(1) obligates public authorities to ensure records preservation in a manner that enables access for the public.

Notably, the thrust on open data sharing and government initiatives like the Draft Data Sharing and Use Policy 2022, assume that collations of data are readily available within government departments. However, these collations are predicated on sound record management, wherein distinct data points and indices are created based on files and records catalogued and indexed prior to the data collation exercise. In this sense, records management is critical to digitisation thrusts of the government that rely on data-based services and policy making to drive the economy.


Using e-office, information management systems, etc for:
- Creation
- Classification
- Destruction/ Archiving
- Storage
- Retrieval
Management
Access
- Classification of accessibility – open/ restricted/ unavailable
- Open information portals, RTI responses and public archives
- Judicial and administrative orders

Despite the thrust towards transparency of governance within the RTI Act and ongoing e-governance initiatives, public availability of public records remains highly constrained. This lends to an incorrect popular perception that governmental transparency encompasses a narrower scope of records.

These fetters emerge from (a) low capacity or will to manage and enable access to records, (b) inadequate enforcement of proactive disclosure requirements under the RTI Act and the management protocols under the PRA, and (c) loose interpretations of exceptions to information sharing under the RTI Act, Official Secrets Act, internal departmental manuals, etc.

Another concern in this regard focuses on metadata, wherein information regarding files created, discussed, etc at individual officer levels is not necessarily available. A discussant cited an interesting best practice in this regard under the erstwhile *Tottenham* system of office procedure and management, wherein officers and clerks were mandated to maintain diaries and registers of all files addressed by them.[11] These diaries served as the record of action items and files received

[11] The Tottenham system refers to a filing system introduced in the colonial era Indian Civil Service (ICS), which continued to be used in the Indian government until it was done away with by individual departments and government

for decision-making by individual officers and clerks within the government, serving as the 'metadata' of government activities.[12]

Thus, the following key recommendations emerged from the discussions here: (i) public records cannot be narrowly defined, accounting for the fact that 'metadata' and records pertaining to a choice not to act are relevant, (ii) public records need to be understood through a classification matrix for improving management and access.

### Governance of Public Records

#### *Singular versus Multiple Governance Frameworks*

Public records governance and management is dispersed across various policy frameworks, statutes, IT protocols and internal departmental procedures. As one discussant pointed out, the dispersed nature of information management under the diversity of e-governance and public digital services is demonstrable through an overarching dashboard – *eTaal* – which records nearly half a billion transactions across the 4000 odd services hosted on it for the first week of April 2022 itself. It was thus suggested that while an overarching governance framework for public records is possible, it must nevertheless account for specificities of distinct initiatives and systems.

Furthermore, overarching public records frameworks need to account for existing management practices and evaluate how these can be realigned (where needed) with overarching principles and frameworks effectively. For instance, the issues of privacy and security cut across schemes and departmental activities. At the same time, it is common practice to display beneficiary lists and records on display boards and blackboards of local offices under the land records and public distribution systems in India to enable accessible monitoring of these schemes at the last mile level. These practices will need to be factored into broad central level frameworks, which may view individual privacy in stricter terms.

#### *Federal and State level management differ*

Public records management is governed under several distinct frameworks at the federal or central level in India, depending on the programme under which records are being generated (e.g, land records digitisation, National Digital Health Mission, etc), or the purpose attributed to the management of the records (archiving, access to information, or file management, etc). Constitutionally, too, records management responsibilities are allocated distinctly[15] and concurrently[16] the Central and State levels. Accordingly, different states have their own way of keeping land records, where land records digitisation programmes have been in different stages of implementation and conceptualisation across states. One discussant specifically highlighted that the Records of Rights (RoRs), which registers the rights and liabilities associated with pieces of land, are variably considered public records across states. Furthermore, different states define land

offices as per their policies. See *Government to bid adieu to Tottenham system*, THE NEW INDIAN EXPRESS, July 1, 2011, available at https://www.news18.com/news/india/government-to-bid-adieu-to-tottenham-system-380729.html.

[12] Ashok V. Desai, *Long Live Tottenham - The enduring merits of the colonial filing system*, THE TELEGRAPH, June 11, 2013, available at https://www.telegraphindia.com/opinion/long-live-tottenham-the-enduring-merits-of-the-colonial-filing-system/cid/293119.

[15] Entry 67, List I, Seventh Schedule, Constitution of India, 1950; Entries 12 and 45, List II, Seventh Schedule, Constitution of India, 1950.

[16] Entry 12, List III, Seventh Schedule, Constitution of India, 1950.

records distinctly, owing to differences in historical practices for land measurements, and patterns of land ownership and land use.[18] Their availability for the public is also determined based on the states' distinct land records programmes. For instance, some states provide encumbrance certificates[19] and RORs openly online, others require a registration/ login before allowing access, while others provide these on a payment basis and may even provide physical copies alone. To be sure, regardless of their nature of public availability, they will qualify as public records, but the manner in which access to them is contemplated, changes.

Similarly, access to records on a particular issue or action – say, access to vaccination statistics – can routinely involve the need to approach departments and agencies across the state and central levels. This experience is shared at the level of the United States as well – while states have their own public records management frameworks, the Presidential and some Congressional and Federal records are managed by the federal agency, NARA. Thus, there is little scope for cohesion of records management between different levels of the government.

### Digitisation of Government Functions

The management of digital public records depends heavily on the IT systems used. The Indian government has increasingly begun adopting ecosystem-level digitisation initiatives such as the Ayushman Bharat Digital Health Mission Stack and India Enterprise Architecture Framework. These systems are designed to include privacy, security, open access, and federated information management principles within their *technical architecture*.

However, these are not complemented by enforceable legal governance frameworks.[20] In this regard, a discussant highlighted that while retrofitting governance frameworks may be possible, developing such frameworks alongside IT integration is a better approach. Further discussions with stakeholders from the IT design industry also support that reconfiguration of IT designs to integrate prospective governance models leads to significant additional expenditure, which can be avoided through the former approach.

#### ***Co-opting the private sector is necessary***

Governments and their agencies are increasingly relying on collaborations with the private sector to manage their records and integrate IT systems within their functions. While the bulk of the Indian government's IT systems rely on those developed or managed by the National Informatics Corporation (NIC), they nonetheless routinely engage private sector vendors to manage databases, develop apps and citizen-facing portals, store information, etc. For instance, the MeghRaj initiative of the MeitY empanels private sector cloud vendors for use of cloud computing services by government departments.[21]

[18] Land Records Modernisation: State-Level Experiences, IIHS POLICY BRIEF (2017), available at http://iihs.co.in/knowledge-gateway/wp-content/uploads/2017/11/2.-State-level-Experiences.pdf.

[19] A legal document certifying if and which legal or financial charges or transactions exist on a piece of immovable property.

[20] *A flawed idea of InDEA!,* INTERNET FREEDOM FOUNDATION, February 26, 2022, available at https://internetfreedom.in/a-flawed-idea-of-indea/.

[21] *GI Cloud (MeghRaj)*, Ministry of Electronics and Information technology, available at https://www.meity.gov.in/content/gi-cloud-meghraj.

In the context of public records and their digitisation, the sheer volume of records poses a significant challenge for the government's IT systems. Citing the experience of the US NARA, one discussant highlighted the overwhelming volume of information managed at the government level as one key reason for the NARA's decision to engage private cloud vendors to manage their archives. At the same time, the discussant also highlighted the following challenges associated with private sector engagements –

*(i) Private Sector Access to Public Information*

Where private vendors are engaged, it raises concerns regarding the propriety of the private sector accessing public information, the terms associated with such access and the propriety of the on-boarding process where public procurement principles and laws need to be complied with. An associated concern is that the capabilities to monitor unauthorised use and monetisation of the same information by private vendors are limited, either during the engagement or beyond it.

*(ii) Limits to platform interoperability*

Platforms for managing and accessing records may also be designed by the vendors providing other services. This leads to path-dependency, where the platforms need to be redesigned according to subsequent vendor engagements. This can also create challenges with capacity building among personnel responsible for engaging with the platforms. Furthermore, different vendors may be engaged at central, state or local levels. Here again, lack of interoperability and standardisation of information management needs to be factored in especially where access must be contemplated in a seamless manner.

Thus, while the government may be compelled to seek support from the private for-profit and non-profit sectors in digitising archives, information management, platform design and the like, it is necessary to account for (a) compliance with public procurement processes, (b) the scope to contractually or legislatively bind external vendors to secure against unauthorised use, access and monetisation by them, and their enforcement, (c) standardisation across central, state and local levels for platforms and management of information, and (d) scope to train and retrain relevant personnel using associated platforms and software.

### ***System design needs a decentralised and people-centric approach***

The design of information management systems has a direct impact on the way that information is accessed by the public: inbuilt access restrictions and protocols, ordering and cataloguing of information, the associated metadata and the choice of file formats influence who and how one can access the record. Crucially, a bulk of the e-governance and digitisation push in India aims to democratise access to services and government functions, improve the disbursal of benefits by plugging leakages, and ensure accountability and transparency of government action.

In this regard, discussants have highlighted several instances of mismatch between these objectives and the design of the scheme. For example, one discussant highlighted an instance where government officials monitoring the implementation of a welfare scheme failed to identify the beneficiaries of the scheme despite quoting a success rate of 80 per cent in fund disbursal, demonstrating the lack of people-centricity in digitisation initiatives at the governmental level. Specifically, the following specific considerations were highlighted for designing people-centric digitisation and information management systems:

*(i) "Public" is a heterogenous term*

When designing management systems to augment public engagement, it is important to note that the 'public' cannot be understood through a singular lens. They differ widely based on their geographical and socio-economic positioning,[22] which determine their levels of comfort in accessing digital infrastructure (such as Common Service Centres, the internet, digital literacy, linguistic literacy, etc) when devising access mechanisms and e-governance solutions.

*(ii) Centralisation of systems decreases individual agency*

The Aadhaar scheme has become predominant in enabling public service delivery through digital means. Case in point, the disbursal of wages through the Mahatma Gandhi National Rural Employment Guarantee Scheme (MGNREGS) is undertaken based on Aadhaar authentication. In case of discrepancies in payments or authentication at the ground level, beneficiaries need to approach local level officials to raise grievances and seek solutions. However, as a discussant highlighted, local level officials, at panchayat and block levels, find themselves disempowered owing to the technical complexity of digital authentication systems, and they may not even have access to login credentials to be able to serve such local grievances. In such cases, individuals may need to travel long distances to reach district level offices, where they can hope to look for solutions. This disintermediation further takes away their socio-cultural capital with local level officials leading to a loss of agency and access that may have been possible within the local village or block levels.[23] Discussants, thus, opined that digitisation initiatives further need to factor in the need for local assistance, and other viable alternatives to disintermediation must accompany large-scale digitisation schemes.

*(iii) The public's understanding of the scope of public records is limited*

Another consideration for system design stems from the inability of the public to imagine the scope of information that can be sought from public institutions. One discussant highlighted that a large proportion of the freedom of information requests (analogous to the RTI machinery in India) in the United States are received for information that is already public. In their experience, the public doesn't always know how to frame queries or know which documents they seek.

Parallelly in India, these discovery challenges manifest in the absence of machine readable and usable public information. In a later discussion regarding the analogous RTI framework in India, another discussant highlighted that much of the information sought through RTI requests is often information that should already be public as per disparate obligations under the RTI and distinct statutory frameworks. Thus, in India, the information asymmetry problem has two layers – (i) not all information is public, despite it being mandated to be public, and (ii) not all information is easily discovered, even when it is public. While this appears to be an access issue, there is a crucial

[22] See Grace Carswell and Geert De Neve, Paperwork, patronage, and citizenship: the materiality of everyday interactions with bureaucracy in Tamil Nadu, India, JOURNAL OF THE ROYAL ANTHROPOLOGICAL INSTITUTE (N.S.) 26, 495-514 (2020), available at https://rai.onlinelibrary.wiley.com/doi/pdf/10.1111/1467-9655.13311.

[23] See Hartej Singh Hundal, Janani AP *et al*, *A Conundrum of Efficiency And Inclusion: Aadhaar and Fair Price Shops*, 55(14) EPW ENGAGE (April 4, 2020), available at https://www.epw.in/engage/article/conundrum-efficiency-and-inclusion-aadhaar-and, and Thomas Chambers, *'Lean on me': Sifarish, mediation & the digitisation of state bureaucracies in India* (July 6, 2020), available at https://journals.sagepub.com/doi/full/10.1177/1466138120940755.

management component to this i.e., public records must also be recorded, indexed and tagged effectively to enable access and discovery.

## II. SYSTEMIC EXPERIENCE OF RECORDS MANAGEMENT

The systemic experience of digitisation and records management in India has largely been documented to reveal capacity, skill and technology deficits, alongside absence of enforcement. This has been attributed to major differences in digitisation levels; lack of reliable records; and limitations on accessibility for the public and for government departments seeking information vis a vis distinct issue.

At a first principles level, a discussant opined that land and property management to secure property and ownership is a primary function of a sovereign. Challenges in management of records reflect a continuation of the ongoing nature of shortfalls in governance processes on this. In this scheme, digitisation represents one mechanism through which governance is carried out. Thus, it is important to approach the issue of records management by also recognising linkages with broader governance frameworks at the meta level, and not divorced from it.

Nonetheless, the discussion delved deeper into the capacity and approach challenges, and highlighted a few specific issues that need discussion while seeking to streamline records management at central and sectoral levels.

### Authentication and repudiation entail further complexities

Non-repudiability and treating a digital document as the single source of truth is a core tenet of digitisation. This accords it legal sanctity, enabling stakeholders to trust the action, rights or obligations contained within the document to be legally enforceable, as well as its source.

Authentication of digital records is undertaken through cryptographic techniques, digital signatures and registration, which are also standardised under rules prescribed under the Information Technology Act 2000. The IT Act also recognises the legal validity of electronic records, thereby granting them the same legal status as paper-based records or documents.[24]

While the legal and technical standards are defined under the law, the following policy complexities emerged from the discussions:

*(i) Digital records exist alongside paper-forms and other digital records:*

Digital records are often from a physical paper-form record that is signed, scanned, uploaded and thereafter, digitally signed. This adds an additional layer, creating challenges with verifying authenticity, where the paper-form record and the digital record may have discrepancies. One discussant cited mutation deeds as a common example in land records wherein such discrepancies between the digital and paper form documents are found. Additionally, owing to differences in policies on how to record information, discrepancies between two types of digital records is also common. For instance, in land records, textual records (RoRs) and spatial records (cadastral maps) can vary on the land area denoted. The digitisation of textual records has also outpaced that of spatial records, where maps are based on outdated land surveys. There is no clarified protocol for resolving discrepancies, and one may nevertheless be more accurate than the other in any given case.

[24] Section 4, Information Technology Act 2000.

*(ii) Human error persists within digitisation initiatives*

Digitisation commonly entails manual entry, wherein human error in recording documentation cannot be eliminated. Digitisation of land records, specifically, has yielded experiences wherein such erroneous registrations are commonplace – arising out of low capacity among data entry operators, *mala fide* registrations motivated by graft etc, inevitable human errors, as well as inconsistent land measurement practices over time and place. Similarly, the legal information management & briefing system (LIMBS) requires manual entry of court records, implemented by personnel with insufficient training and capacity to implement legal stipulations in this regard.

While these concerns may not universally arise in certain sectors, these appear acute in certain other sectors like land records management. Furthermore, encryption-based authentication is fallible where (a) security breaches are still possible, and (b) actors involved in the breach cannot be held accountable under existing laws. At the same time, discussants have argued that digitisation has enabled the use of complementary technologies and records that can be used to corroborate claims better. In this regard, one discussant cited the use of cadastral maps alongside the registration and record of rights documents to assess land ownership claims. Further investigation of this issue has highlighted that government departments of land, revenue and survey are not necessarily involved within land records digitisation programmes, which can exacerbate problems associated with difference in textual and spatial data.[25]

**Limitations on implementation and accountability**

Public records digitisation faces several implementation challenges, which hinder the ability to access public information, secure service delivery and seek accountability of action. As part of the discussion, panellists identified the following specific challenges:

*(i) Lack of clarity regarding supervisory authority*

Digging deeper into the challenge of fragmented laws and policies, one discussant specifically highlighted the dissonance between different central departments implementing and overseeing digitisation of government functions as a key challenge towards guiding policy making and securing implementation of protocols. Specifically, according to the Allocation of Business Rules, the following overview of competing frameworks becomes evident:

| S. No. | Ministry/ Department | Allocation[26] | Implementation Experience |
|---|---|---|---|
| 1. | MeitY | (i) Assisting other departments with e-governance, e-commerce, e-infrastructure etc.<br>(ii) Administration of IT Act, thereby formulating rules for maintaining the public key infrastructure, status of digital | MeitY has developed e-office suite for digital file management, standards and guidelines for, *inter alia*, the use of email, digital devices, and enterprise architecture, and formulated rules for the public key infrastructure in India. |

[25] *Land Records Modernisation: Institutional Interfaces*, IIHS POLICY BRIEF (2017), https://iihs.co.in/knowledge-gateway/wp-content/uploads/2017/11/4.-Institutional-Interfaces.pdf.

[26] Government of India (Allocation of Business) Rules, 1961, Constitution of India, 1950.

| | | | |
|---|---|---|---|
| | | signatures and records, etc.<br>(iii) UIDAI - agency administering the Aadhaar infrastructure, which forms the backbone of public service delivery in India. | |
| 2. | Ministry of Information and Broadcasting | (i) Oversight of digital online media - including social networking websites. | Under the new IT Rules, online media is regulated through a content code and intermediary guidelines by both MeitY and MIB. |
| 3. | Department of Administrative Reforms and Personnel Grievances | (i) Administration of Central Secretariat Manual of Office Procedure<br>(ii) Administrative Reforms, including e-governance and dissemination of best practices | The digitisation of records is nevertheless dictated by MeitY's e-filing system. The record retention schedule and the manual of office procedure are not updated to reflect common communication media used within governmental decision making |
| 4. | Ministry of Culture | (i) Oversight of the Public Record Act, 1993 (PRA)<br>(ii) National Archives of India (NAI) and Gazetteers | The primary records management law continues to be the PRA. However, the implementing agency is the NAI. The NAI are digitising their archival records, but the Ministry of Culture and the NAI do not have capacity to oversee digitisation and records management for transparency purposes. |
| 5. | Ministry of Statistics and Programme Implementation | (i) Prescribing norms and standards in statistics, definitions and methodology of data collection, processing of data and dissemination of results.<br>(ii) Oversight of government surveys, public finance reports, audits thereof, etc. | One discussant highlighted that this ministry possibly holds the most capacity to ideate on overarching norms for records management insofar as data collection is concerned. |

Given these overlaps, the actual implementation of records management norms and guidelines is similarly spread across government departments, with variable levels of capacity and scope for formulating laws and guidelines, implementation and oversight, and enforcement. This is further exacerbated where information is sought on specific issues, wherein different line ministries might have jurisdiction. Citing the example of queries on government spending on old age pension, a discussant pointed out that it can span across ministries of social justice as well as expenditure. These overlaps further enable public offices to evade responsibility where public queries can be deflected to other departments and authorities, limiting public access to such information.

*(ii) Limited enforceability under fragmented laws*

No enforcement is contemplated under laws for the quality of information management and sharing under each department. Furthermore, the laws are disaggregated and vaguely defined. Notably, one discussant with experience as a government official cited that data officers tasked with uploading data onto the government open data platform (data.gov.in) do so entirely on their own initiative. These responsibilities arise from the National Data Sharing and Accessibility Policy 2012, which does not create enforceable duties. Similarly, the MeitY released the E-mail Policy of India 2014 and accompanying Guidelines to specify the government's use of emails. One discussant highlighted that despite a Delhi High Court order (and a stipulation within E-mail Policy[27] and Guidelines) that government emails be hosted on NIC servers, government departments continue to use private servers for email-based official communication.

*(iii) Scope of frameworks does not sufficiently include new modes of communication and decision making*

Decision-making within governments has increasingly moved to instant communication platforms like WhatsApp. These increase efficiency in terms of quick decision making but from an accountability perspective, create opacity of government functioning. This is because these are not specifically covered by the Manual of Office Procedure which lays down procedures for how government records and files need to be shared, retained and managed. Additionally, for WhatsApp conversations to be considered public, device and the phone bill should be paid for by the government.[28] This excludes public officials making decisions on WhatsApp installed on their personal phones, which is the norm. Additionally, several states continue to follow dated manuals and guidelines dating to the colonial Indian government, which cannot guide management for newer technologies.

*(iv) External engagements limit public oversight*

In several instances, government agencies and departments engage external partners to build and maintain information management systems (MISs). In these scenarios, while the government is engaged in the development process, the final execution of these systems is undertaken by engineers, who are not primarily driven or bound by public duties and considerations. Therefore, there is no guarantee or accountability attachable for determining what is publicly relevant to be

[27] Para 2.1, E-mail Policy of India 2014.

[28] In the United Kingdom and Australia, the Information Commissioner's Offices have undertaken reviews of the use of WhatsApp conversations within governments and treated such communications as a matter of public record. See *"Behind the screens – maintaining government transparency and data security in the age of messaging apps"*, REPORT OF THE INFORMATION COMMISSIONER TO PARLIAMENT (July 2022), available at https://ico.org.uk/media/about-the-ico/documents/4020886/behind-the-screens.pdf; See also Doug Dingwall, *WhatsApp conversations with ministers, bureaucrats should be recorded: National Archives boss,* CANBERRA TIMES, April 15, 2021, available at https://www.canberratimes.com.au/story/7209152/public-servants-should-log-whatsapp-conversations-archives-boss/.

documented and managed under the MIS. Furthermore, where external partners undertake data entry, public accountability mechanisms cannot check any errors as they do not directly bind individual employees of contracted partners of the government.

**Usability of Records**

Quality and comprehensiveness are essential to records management. Specifically, the manner in which records are collected, retained, digitised and made accessible determine how records are used. The following common issues emerged from the discussion on sectoral experience of public finance and land records management in India:

*(i) Monetisation and Profiling*

Court records and land records are two common instances where digitisation has been implemented at scale. Citing experiences with the same, discussants revealed experiences wherein private actors are keen to gain access to individual level government records. However, these are liable to risks of profiling of individuals, and being monetised by such private actors. For instance, facial and image recognition information is being used not just for detection of crimes and traffic violations, but also insurance purposes.

In such scenarios, it is important to clearly identify the public function performed by such digitisation and publication. Another discussant also highlighted the need for legislative and contractual frameworks to ensure accountability where such use creates such risks for data protection, surveillance and inappropriate monetisation of open public information. This is discussed further under the next chapter on access to information, wherein privacy is discussed more specifically.

*(ii) Indexing and Cataloguing*

Digitisation within the government is supported through a host of technical services. Exemplarily, the e-office suite is launched by the MeitY for government departments to adopt for maintaining internal digital files. While a MeitY official cited its increasing use, another discussant highlighted that such applications nevertheless lack sufficient indexing and cataloguing facilities, which make discovery of files - circulars etc difficult, thereby limiting their usability. On the other hand, a best practice cited in this regard includes the practice of indexing of files maintained as proceedings of Indian Central Ministries between 1940s and 1950s. These served as a mechanism for even officials within the department to understand which files were created in a given year, enabling oversight of government action.

*(iii) Granularity*

Citing the example of public finance disclosures, one discussant highlighted that government information is commonly provided in bulk and aggregated forms. In the context of public finance, accountability necessitates granular information - such as facility-wise allocations, spending and balances. Engagement with budget information has demonstrated that in spite of information being collected at facility levels, digitised records are nevertheless available only up till block levels. In most instances, such data is not available beyond municipality level allocations and spends. In this regard, MGNREGS, which enables beneficiary level tracking and monitoring, and Kerala, where Gram Panchayat level data is available emerge as best practices to study closely.

## III. Access to Information and Limitations Thereto

At the central level, access to public records is variably contemplated under legal and policy frameworks as follows:

| S. No. | Framework | Purpose and Scope |
|---|---|---|
| 1. | RTI Act 2005 | Covers every record of every public authority, and allows access to any person seeking information. It provides for both proactive disclosure mandates as well as responses to RTI queries. |
| 2. | PRA 1993 | Governs the preservation and management of a public record, tracking its entire life cycle, including process and timelines for the retention of the record, but only vis a vis the executive branch of the central government and public sector companies. Access is contemplated only post 20–30 years of its origination to researchers through the NAI. |
| 3. | NDSAP 2012 | Constitutes Indian government's open data policy, setting forth the policy for government departments to share data in a manner that is technologically free, machine readable, not in proprietary formats and free of cost. This is primarily aimed at enabling access to data scientists, researchers, academicians to develop services using this data. |
| 4. | Departmental manuals | For instance, the Central Secretariat Manual of Office Procedure (CSMOP) lays down the e-office procedure, origination of file in the e-office suite, its tracking and retention. It's meant to enable ease of locating files digitally for internal departmental access.<br>Other manuals include the Manual of Departmental Security Instruction, alongside state level manuals. |

Apart from these, distinct sectoral frameworks enable access through websites and application procedures contemplated specifically by the concerned department. These also differ across the scope covered, timelines, contemplated access groups and purposes. Evolving conceptualisations of public interest vis-a-vis the right to privacy, interests in national security, confidentiality and intellectual property further impact access to public records.

### Open Government and Open Data

#### ***Proactive information disclosures remain scarce***

The RTI Act mandates public authorities to maintain, catalogue, index, computerise and network all records that they term appropriate to enable access to these records.[29] It further mandates public dissemination of records including, *inter alia*, procedures followed to make decisions, the channels of supervision and accountability, powers and duties of officers and employees, categories of documents held by it, public consultations, budgets, allocations, spending and manner of disbursal,

[29] Section 4(1)(a), Right to Information Act 2005.

execution of subsidy programmes, and the reasons for administrative and quasi-judicial actions taken.[30]

One discussant with experience with the RTI machinery pointed out that among a sample of 5000 RTI applications, 70 percent were seeking information that should have been actively provided. Within this, 50 per cent would be covered under the proactive disclosure mandate under Section 4 of the RTI and 20 per cent entail information that should have been provided even outside the Section 4 mandate (e.g., the results of a recruitment process).

***Digital divide limits meaningful dissemination***

The dissemination requirement is broadly understood to mean publication on government websites, even though several other mechanisms such as newspaper publications are also enlisted in the Act. This restricts meaningful engagement given that digital divide is a crucial characteristic of Indian society, and the internet is not accessible to a large section of the society. There are additional generational divides and gender divides that arise given the lack of digital literacy, access to devices and autonomy, which limit meaningful access to internet and mobile based public information.

In response, helpdesks in local and corresponding government offices, availability of personnel at the Common Service Centre (CSC) levels were cited as policy solutions. Discussants also pointed out examples of government portals which provide real time, village level information as best practices for disseminating information electronically. These include (i) Koshvani[31] in Uttar Pradesh hosting real time data of government spending in the state, including allocation of budget, for which line item, salaries etc., and is designed to be bilingual; and (ii) Adigrams[32] (Adivasi Grants Management System) providing up till village level data on tribal welfare schemes, to show how budgets are being used and where gaps lie to enable accountability.

***Nuancing the balance between public interest disclosures and privacy***

The open data experience has revealed that the balance between privacy and public data sharing is hard to find in India - teetering between unnecessary and harmful personal data sharing or complete withholding of socially relevant data.

For instance, Aadhaar information containing personally identifiable information is commonly made public, as also ration cards and BPL numbers, which are published in a manner that creates clear reidentification and privacy risks. Similarly, the dashboard of the Jal Jeevan Mission shows on ground locations of households on geospatial maps as part of household level data, which can create privacy risks, without having shown clear use cases for such geo-spatial imagery. Another cause for concern is traced to the publishing of court records, wherein disputes and cases containing children's personal information are shared without redaction. The discussant cited that a study of best practices in this regard undertaken by Macquarie University and the HAQ Centre demonstrates that Canada, Australia, US, UK, Malaysia, Singapore are among a few countries where judicial data is released post redacting children's names, and some also employ strong non-

[30] Section 4(1)(b) and 4(2), Right to Information Act, 2005

[31] *Koshvani*, available at https://koshvani.up.nic.in/KoshvaniStatic.aspx.

[32] *Adivasi Grants Management System (ADIGRAMS)*, available at https://grants.tribal.gov.in/adigram.

identifying features.[33] In India, however, district courts in Delhi, Assam etc are commonly published without redacting children's names. On the other end, courts have stopped publishing cases under the Protection of Children from Sexual Offences Act, 2012 (POCSO) altogether, as not all e-courts are able to comply with privacy norms.

On the other hand, while the mainstream understanding of data protection principles would imply that names and addresses of beneficiaries should not be publicly released, social audits for welfare schemes like PDS necessitate, and are in fact predicated, on such disclosures. In such instances, discussants stated that there is a need to evolve privacy norms based on the society that we live in. Particularly, the individual-focused idea of privacy needs further nuance to integrate the importance of '*collective negotiation of rights and entitlements*'. There is a case to be made to integrate the notion of '*community access to information*', where such personal information is not necessarily available to the world at large, but to a limited set of people within a community.

As such, the discussant opined that the way we approach the question of public disclosures should be nuanced to account for the public purposes for which information is needed. For instance, voter information is public, and people routinely disclose personal information to access critical services (e.g., while sourcing medical supplies and hospital beds during the second wave of the COVID 19 outbreak in India). Therefore, every disclosure of personal information does not constitute a breach of privacy and must be evaluated through the lens of the purpose behind disclosures, the time for which it was disclosed, and the medium used.

### *Addressing IP and Confidentiality*

Public bodies' claims to ownership of public information are a key contention within the open government movement. One discussant pointed out that experience demonstrates that IPR protection has been loosely interpreted to restrict access to public information. Specifically, they cited that the Bureau of Indian Standards (BIS) publishes standards which are mandatory to be followed by manufacturers. These standards operate like a law and should therefore be easily accessible in the interests of informing manufacturers of their legal obligations as well as consumers of their rights against the manufacturers. It is also arguably covered under the stipulations of section 4 of the RTI, mandating disclosures by public authorities.[34] However, copies of standards are made available only on payment basis, based on a claim that they are protected from publication under copyright law.[35]

Another such example is the withholding of information regarding classification of files within the government. Agencies covered by the PRA are required to undertake reviews every six months

[33] Kane Elder, Maddison Tan et al, *Balancing Children's Confidentiality and Judicial Accountability: A Cross-Country Comparison of Best Practices Regarding Children's Privacy in the Criminal Justice System*, HAQ CENTRE FOR CHILD RIGHTS AND MACQUARIE UNIVERSITY, available at https://www.haqcrc.org/new-at-haq/balancing-childrens-confidentiality-and-judicial-accountability.

[34] Prashant Reddy, *Copyright in "Standards": Taking a look at the PIL by Malamud, Sinha & Kodali against BIS*, SPICY IP, February 17, 2017, available at https://spicyip.com/2017/02/copyright-in-standards-taking-a-look-at-the-pil-by-malamud-sinha-kodali-against-bis.html.

[35] Naveena Ghanate, *Indian standards still inaccessible to people*, DECCAN CHRONICLE, August 16, 2018, available at https://www.deccanchronicle.com/nation/current-affairs/160818/indian-standards-still-inaccessible-to-people.html; Anuj Srivas, *Interview: 'This Little USB Holds 19,000 Indian Standards. Why Should it Not Be Made Public?'*, THE WIRE, October 26, 2017, available at https://thewire.in/tech/interview-little-usb-holds-19000-indian-standards-not-made-public.

regarding their management practices, the records that are declassified, etc. A discussant stated that except for MeitY, none of the other departments share such reports. Furthermore, in response to an RTI query seeking information on the number of records classified as secret, top secret and confidential, the government has responded that such information is not available with the government. The basis on which they are thus classified i.e. the Manual of Departmental Security Instruction is also not available for public release.

Furthermore, a discussant shared that based on their investigation of this issue, a verbatim copy of these instructions is available in another public document - the 'security instructions' chapter in the Andaman and Nicobar Manual of Office Procedure, under which classification of documents as secret (and therefore withheld from public view) is based on criteria as vague as the likelihood to cause "*administrative embarrassment or difficulty*" among other reasons.[37] This is also the category of documents, which is designated to be "*ordinarily used for very important matters*".

### *Fetters to open licensing principles*

Open sharing entails ease of access, free of charge, with no fetters on its use and repurposing. While public information should ideally be shared openly, there have been instances where once information is uploaded onto government websites, access to information is restricted through password protected logins.

The NDSAP 2012 indicates a framework for government data to be uploaded by individual departments and ministries onto the government open data portal. Central ministries, however, upload datasets in volumes that are disproportionately low compared to the number of datasets they are likely to be holding. For example, Rajya Sabha has uploaded about 16000 datasets, which do not account for the number of questions received and the answers thereto, all of which should ideally be collated. State governments similarly upload a much lower number of datasets, with Delhi having uploaded a total of four datasets.

Other issues highlighted by a discussant include:

(a) Datasets are not contemporaneous; most datasets are out-dated and static in nature;

(b) Chief Data Officers tasked with uploading data are commonly not appointed;

(c) Data fields and metadata are often missing;

(d) High value data sets are not available;

(e) Capacity to upload and manage data is limited; and

(f) Systems and data sets do not cater to native language users as these datasets are not multilingual or bilingual.

Exemplarily, experience has shown that there has been a reluctance to share data by the Ministry of Finance in the past two years in Excel format, by citing other departments as the source. Similarly, COVID-19 related data had to be sourced from the open data community by the Economic Survey in India 2021-22.

[37] Draft Manual of Office Procedure, Andaman and Nicobar Administration, 2008, available at https://www.humanrightsinitiative.org/programs/ai/rti/india/national/2009/email_alerts/MODSI-Andaman-DraftMOP-TOCChap13-2008.pdf

## Implementation of the RTI Act

Section 8 under the RTI Act provides several grounds for exempting information disclosures, though public interest is a common thread for determining whether the exemption applies. Of these, the workshop focused on privacy, confidentiality and intellectual property exemptions. The discussions for each highlighted dissonances in the application of the RTI Act and the exemptions cited.

### *(i) Burden of proof*

The public information officer (PIO) holds the burden of proof in justifying why exemptions apply and therefore the information cannot be released. However, discussants stated that in their experience, the PIOs and departments commonly require the querists the reason for asking for such information in an often-informal process.

### *(ii) Speaking orders*

A reasoned order needs to accompany RTI responses as per the RTI Act. However, PIOs provide a negligible number of orders in speaking order form, leading to opacity of the reasons for which information was denied under an RTI query. This also restricts the ability of individuals to appeal against these orders.

### *(iii) Appointments to Information Commissions*

Discussants highlighted that the appointments to information commissions are often politically motivated, lacking justification based on their qualifications. In other instances, Information Commissions lie defunct owing to a failure to appoint any Commissioners to them - e.g., Jharkhand, Tripura and Meghalaya Information Commissions.

### *(iv) Overt exemptions from the RTI framework*

There are also instances where funds and bodies are designed in a manner that they become exempt from the ambit of public authorities under the RTI Act. Instances cited include the PM Cares fund, which was retrospectively changed to fall outside that ambit of 'public authorities'. Simultaneously, the related CSR rules were amended to enable the fund to fall outside the scope of RTI while retaining the ability to receive CSR funds (which would otherwise not be possible for other non-public authorities).

## ***Balancing Public Interest and Exceptions to Information Disclosures under the RTI Act***

Exemptions under the RTI Act are contained under Section 8 and 9, spanning invasions to privacy, confidentiality, protection as a trade secret, etc and the impact on individual copyright interests respectively. The erroneous interpretation applied to a proviso Section 8(1)(j) on privacy, which states that information cannot be denied citing the exemption if this information is also available with the State or Central Legislature emerged as a major challenge. Discussants pointed out that this proviso is commonly misunderstood by PIOs to apply to the last clause of the section, even though the original drafting seeks to apply the proviso to the entire section, covering all exceptions. This error has the effect of extending the scope of the other exemptions, and concomitantly reducing the scope of the right to information under the Act.

The discussions also brought forth specific perspectives and experiences with the balancing exercise undertaken by Public Information Officers (PIOs) and Information Commissioners in the context of privacy and intellectual property and confidentiality, which are discussed further in the sections below.

*(i) Privacy*

The RTI Act exempts that personal information, whose disclosure is not related to any public activity or interest, or which would invade privacy of a person in an unwarranted manner, provided a public interest justification exists. Furthermore, if such information has been made available to a State or Central Legislature, then it cannot be denied on the basis of the privacy exemption to an individual seeking the information.[38]

In practice, this provision is applied using overbroad interpretations of privacy that would fall foul of the public interest balancing required under the section. Specifically, one discussant opined that the Supreme Court in *Girish Ramchandra Deshpande v. CIC* (2013) 1 SCC 21 erred in interpreting the section without accounting for the provisos therein. This has resulted in reducing the ambit of public information, as Information Commissions and PIOs commonly follow it as precedent. Foremost, it needs to be reconciled with the holding in *R. Rajagopal v. State of Tamil Nadu* 1994 SCC (6) 632, and *Justice KS Puttaswamy v Union of India*, which limits the right to privacy in records once they become public. The broad interpretation of the privacy exemption has been invoked to thereby deny information on performance reviews of IAS officers,[39] funds of Members of Parliament, assets of public officials[40], and even the details of the government's contract with Bharat Biotech for Covaxin production[41].

In another instance, a discussant cited that in a query seeking the order of the Collegium in 2018, the Supreme Court's PIO cited S. 8(1)(j) as a residual exemption that would apply - implying that anything pertaining to a person would be covered within the scope of this exemption.

*(ii) Intellectual Property Rights and Confidentiality*

Under sections 8(1)(d) and 9 of the RTI Act, intellectual property rights, commercial confidentiality and trade secrets, and copyrights respectively exempt information disclosures to the public. Discussants highlighted that these exemptions are loosely interpreted, similar to the privacy exemption, to grant wide exemptions from such disclosures. Exemplarily, RTI queries seeking details of the agreement between Bharat Biotech and the government for the production of Covaxin, and the royalties claimed, were denied information on grounds of commercial interests of the manufacturer.[42] Similarly, in another case seeking question papers and answer keys for exams conducted by a public university, the concerned PIO cited intellectual property-based exemptions

[38] Section 8(1)(j), Right to Information Act, 2005

[39] Dr. Nutan Thakur v. CPIO, CIC/DOP&T/A/2018/172993 (2021), available at https://indiankanoon.org/doc/108926546/

[40] V. Madhav v. The Tamil Nadu Information Commission and Anr. W.A.No.551 of 2010, available at https://indiankanoon.org/doc/185136737/

[41] *ICMR denies Covaxin's MoU and Funding Details under the RTI Act*, SOFTWARE FREEDOM LAW CENTRE, July 5, 2022, available at https://sflc.in/icmr-denies-covaxins-mou-and-funding-details-under-rti-act.

[42] *ICMR denies Covaxin's MoU and Funding Details under the RTI Act*, SOFTWARE FREEDOM LAW CENTRE, July 5, 2022, available at https://sflc.in/icmr-denies-covaxins-mou-and-funding-details-under-rti-act.

to deny the information to the querist. This was later overturned on appeal, holding that disclosure is the norm, while withholding information is the exception as per the RTI Act.[43]

[43] Mr. Mangla Ram Jat v. Banaras Hindu University, CIC /OK/A/2008/00860/SG/0809, available at https://indiankanoon.org/doc/1575964/.

## KEY TAKEAWAYS AND NEXT STEPS

Based on the discussions across the two-day workshop, we have synthesised takeaways that can help inform the next set of research outputs envisioned under the Project. These are discussed below.

### *(i) Definition and Scope*

The definition of public records should remain inclusive and broad covering all public authorities. At the same time, universalisation of classification and concomitant availability to public is necessary. These should be defined in a purpose specific manner, using clear classification of documents to convey their availability for public dissemination.

### *(ii) Governance frameworks*

The current set of governance frameworks are disaggregated and hold varying degrees of prioritisation vis-à-vis access, sharing, preservation and use. They are also differentially enforceable. At the same time, sectoral initiatives like digitisation of land records and public finance have specific challenges that may not apply universally (e.g., authentication and duplicity of records). In such a scenario, an overarching, binding law will not be able to address specific challenges that cut across sectoral idiosyncrasies and priorities. Instead, binding principles at a central level, alongside sector and domain specific laws, which are guided by a supervising ministry or authority would be better suited to address the fragmentation as well as sectoral priorities. These principles can also be accompanied by model protocols to enable better guidance.

Furthermore, the scope of existing governance frameworks needs to be revised to incorporate new methods of correspondence and decision making (e.g., WhatsApp, email, Twitter) to bring these within the scope of accountability and transparency extended to other public records.

### *(iii) Data Protection and Privacy*

Privacy is an issue that cuts across management and access challenges identified. Specifically, the emphasis on protecting disclosures of personal information needs to be tempered to account for the community-based nature of Indian society, wherein limited purpose- and time- limited disclosures are often necessary to access essential services (e.g., social audits for benefits under the PDS system). At the same time, privacy needs to be factored into the way that disclosures are made. It is necessary to identify how records disclosures can be made privacy respecting tied to efforts to redact unnecessary information, and identifying how such disclosure serves a public function. There is also a need to decouple the use of personal information for scheme monitoring purposes, and for enabling access to services at the governmental level.

### *(iv) Intellectual Property and Ownership*

The scope of the government to claim ownership over public records and government data is constricted under intellectual property law. However, it is routinely expanded through overbroad interpretations. Furthermore, the custodianship framing of the government's role is not clearly defined and needs further research.

### *(v) The Right to Information Framework*

The right to information framework is technically sound and feasible in terms of the legislative drafting. However, its implementation has been lax owing to capacity and skill challenges, lack of appointments, and skewed implementation of exemptions and proactive disclosure requirements. In this regard, it is necessary to study how the duty to inform is governed under the framework, while simultaneously exploring manuals and implementation handbooks to help PIOs and the like have openly available guidance on making public interest and disclosure determinations.

*(vi) Linkages with Government Data*

Data sharing initiatives are predicated on the availability of comprehensive, updated and collated databases which also rely on sound management of records. As such, open data initiatives and records management are linked. Policy frameworks thus looking towards sound data use and sharing are incomplete in their outlook where record-keeping and archiving are not considered. Further research is identified for assessing these linkages and concomitant legal and policy overlaps.

*(vii) Digitisation needs inclusive approaches*

At a policy level, digitisation has not proceeded in an inclusive manner. There are severe gaps created by the disintermediation of access to e-governance frameworks, disempowering of local level officials who often serve as the only points of contact to a majority rural population, and through assuming capacity and access through inadequate proxies of mobile internet penetration. Keeping the digital divide in mind, digitisation should be complemented with skilled human operators at local levels. Furthermore, public dissemination through internet needs to go hand in hand with other modes of seeking information through CSCs, more ubiquitous communication modes such as phone calls and text messages, engagement of panchayat and municipal offices, and helpdesks to cater to individuals at the ground level.

**Immediate Research Objectives under the Project**

We acknowledge that the scope of research under this project is vast in terms of the governmental levels engaged, as well as the sub-issues that necessitate a study. Thus, based on these discussions, we have identified two narrow spaces within which to locate our future work within this project:

*(i) Focused Case Study*

Evidently, the state of digitisation, the extant information management systems and the law and policy objectives associated with the given government department or agency are essential to understanding public records management vis-à-vis a designated department. Thus, we hope to understand the issues captured within this report through a focused case to inform the project of the law and policy challenges in records management at an empirical level. To this end, we seek to engage with a singular government department, whereby we place these enquiries within their specific stage of digitisation, their governance objectives and duties, and the applicable law and policy landscape.

The details of this engagement will be collated in a subsequent report.

*(ii) Re-establishing the link between data and records management*

The interlinkages between data and records management remain unexplored for India. At the same time, data management is a key part of information laws and transparency thrusts by governments across the world. To this end, we seek to understand the specific ways in which the two are interlinked, and how otherwise distinct records management and government data initiatives can reintegrate these linkages to achieve public transparency objectives for India.