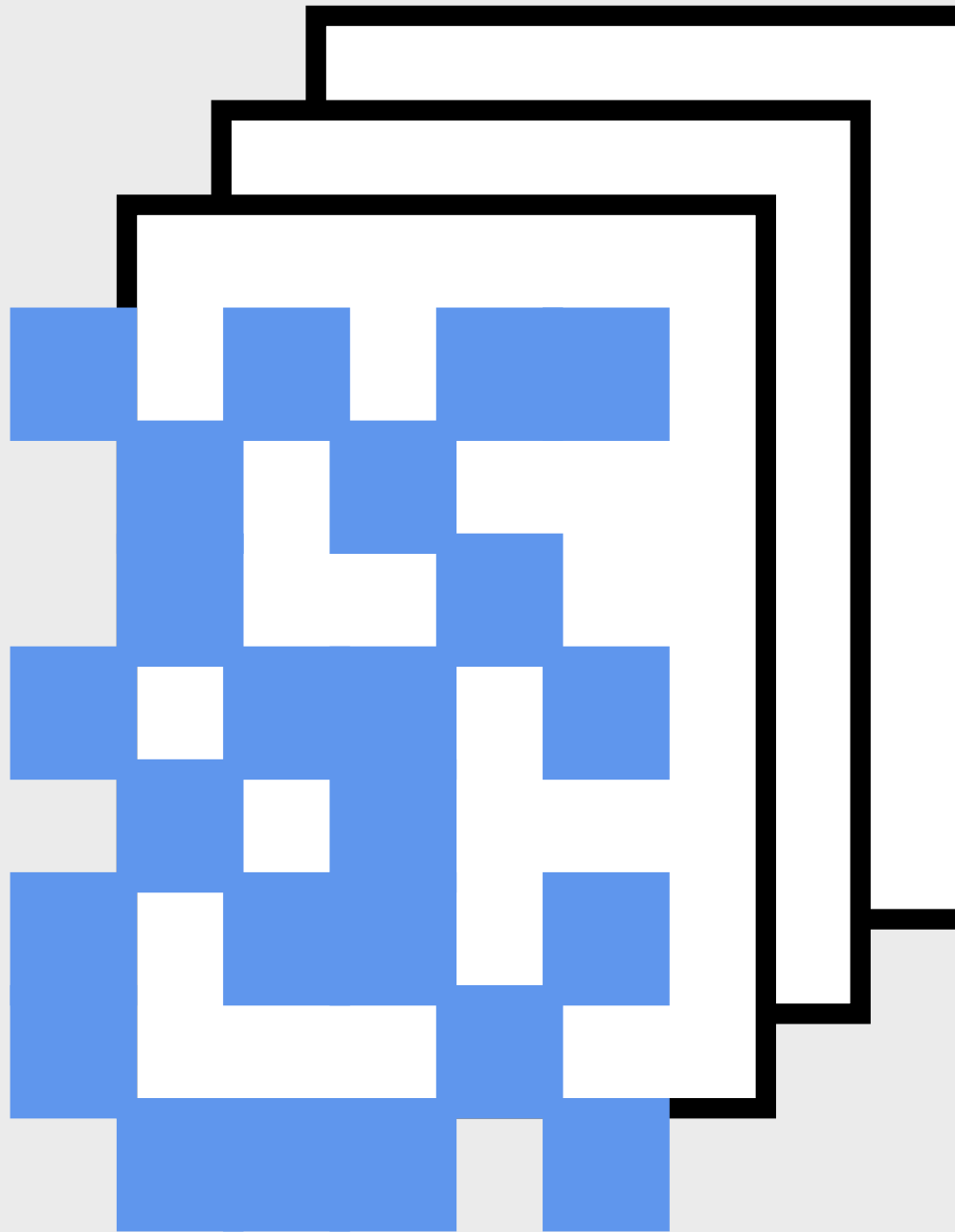


The Digital Veil on Public Records

A Critical Appraisal of
e-Records Governance
in India

Tarika Jain



Funded by

Tarika Jain is a MSc Public Policy student at University College London.

This study has been funded by Thakur Family Foundation.

Contents

	I	
01	Introduction	
	Emergence of New Forms of Records in the Digital Age	02
	II	
05	The Transition to E-Governance: Generating e-Records Today	
	A. Administrative Records: E-Office Project	06
	B. Financial Records – PFMS and GSTN	06
	C. Legal Records : Legal Information Management & Briefing System	07
	III	
09	Legal Framework for Governance of e-Records and Data	
	A. The Public Records Act and the Right to Information Act	09
	B. CSMOP & CSeMOP	10
	C. E-governance standards	11
	D. National Data Sharing and Accessibility Policy	12
	E. Policies and Guidelines Governing Electronic Communications (Emails, social media and websites)	13
	IV	
15	Shortcomings in Effective e-Records Management	
	A. Inconsistencies between the legal framework	15
	B. Lacunae in the PRA	16
	C. Limitations of the Open Data Policy	18
	D. Failure to preserve electronic communications	19
	V	
22	Conclusion	

Introduction

Civic participation in public affairs is the cornerstone of democracy. As the principals of their elected agents, citizens are entitled to monitor the functioning of the government and ensure that their representatives remain accountable for their actions. Moreover, meaningful conversation and criticism can play an important role in improving government efficiency and contribute to public good. For this to happen, it is imperative that the governments are transparent and the citizens have the knowledge of what transpires within the public sector. Access to such information reduces asymmetry and establishes a balance of power between the public and the government. It opens doors for new solutions to problems in governance through public engagement.

In realisation of this tenet of democracy, in the mid 20th century, demands arose from civil society and journalists across the globe for hard measures for increasing transparency. As a result, the Freedom of Information Act was passed in

the U.S. in 1966 which allowed the citizens the right to request for access to records held by any federal agency.¹ Subsequently, the movement for transparency received a significant boost in the 1990s, when owing to strengthening of civil society organisations and greater economic integration across borders, the state agencies around the world were pressured to embrace the open government principle and bring visibility to their processes.²

In India, the Supreme Court, in two of its landmark decisions,³ expressly recognized the citizens' right to know about the affairs of the government, paving the way for sustained transparency efforts in the future. Notably, in the SP Gupta case, the Supreme Court noted that “the concept of an open government is the direct emanation from the right to know which seems to be implicit in the right of free speech and expression guaranteed under Article 19(1)(a).”

1 Ann Florini (ed), *The Right to Know: Transparency for an Open World* (Columbia University Press 2007) 7-8.

2 Ibid 8-9

3 *State of UP v. Raj Narain* A.I.R. 1975 S.C. 865; *SP Gupta vs. The President of India & Ors* 1982, AIR SC 149, 234.

Despite these rulings, there were little efforts on the part of the Indian government to allow citizens a window to its functioning.⁴ Consequently, citizens united at the grassroots to struggle for greater transparency. The most significant of these were the efforts by Mazdoor Kisan Shakti Sanghathan and National Campaign for People's Right to Information which ultimately succeeded in getting the Rajasthan government to pass a right to information law for the state.⁵ While prior to this, the states of Tamil Nadu and Goa had already introduced laws on the subject, the move gave impetus to similar enactments in other states such as Maharashtra, Karnataka and Delhi for their respective governments. Drawing from the experiences of the states, the central Right to Information Act ("RTI Act"), 2005 was enacted after intense campaigning by the proponents of transparency.⁶

The RTI Act guarantees to every citizen the right to request for any public record from a public authority by following a simple procedure. It also makes it incumbent upon the public authority to proactively disclose basic information about its organisation in a periodic and accessible manner. The movement behind the law ensured that the Act had sufficient teeth for effective implementation by ensuring the inclusion of two important safeguards - the first being a penal provision for non compliance by the public officer and the second being an independent appellate mechanism.⁷

While the introduction of the RTI Act provided the vehicle by which a citizen could access information about the public sector, an already existing legislation, the Public Records Act 1993 ("PRA"), provided the framework for public authorities of the Central Government to store this information in a systematic manner. As public records are a key source of knowledge about state activities, containing crucial information, right from the grassroots to the larger interests of the country, their maintenance, organisation and retention is a prerequisite for exercising the hard earned right to information.⁸ Therefore, the implementation of the RTI Act is dependent on the strict compliance of the PRA.⁹

Emergence of New Forms of Records in the Digital Age

In recent years, the government has been hoping to increasingly rely on technology to carry out its day to day work. The National e-Governance Plan ("NeGP"), which was approved in 2006, currently encompasses 44 Mission Mode Projects ("MMP")¹⁰ which target digitising a number of key public functions and services such as taxation, procurement, pensions, e-courts and administration coordination. At the state level too, institutions such as prisons, police, panchayats and municipalities as well as services such as education, health, rural development and women and child development are increasingly operating

4 Florini (n 1) 23.

5 Neelabh Mishra, 'People's Right to Information Movement: Lessons from Rajasthan' (*Human Development Resource Centre*, 2003) 2-3.

6 Aruna Roy and the MKSS Collective, 'Excerpt: The RTI Story; Power to the People by Aruna Roy with the MKSS Collective' (*Hindustan Times*, 13 April 2018) <<https://www.hindustantimes.com/books/excerpt-the-rti-story-power-to-the-people-by-aruna-roy-with-the-mkss-collective/story-V5AWqGRa84dCxYoVsR2o4L.html>> accessed 6 December 2020.

7 Ibid.

8 Florini (n 1) 196.

9 Vidya Venkat, '10 years after RTI, transparency under cloud' (*The Hindu*, 16 May 2015) <<https://www.thehindu.com/news/cities/Delhi/10-years-after-rti-transparency-under-cloud/article7213480.ece>> accessed 6 December 2020.

10 National e-Governance Division, Mission Mode Projects – Complete List <<https://negd.gov.in/sites/default/files/AllMMPS.pdf>> accessed 6 December 2020.

digitally. In the process, voluminous data and digital records are created by officials, ranging from administrative files, financial transactions and even emails and text messages exchanged for official purposes. Owing to the rapidly changing nature of technology, these records and data are generated and collected by the government digitally in formats which were quite unimaginable even two decades ago. For instance, it is even argued that posts on social media accounts held by the government are also digital public records and should be altered or deleted only after following due process.¹¹

In India, the Information Technology Act (“IT Act”), 2000 defines and affords legal recognition to electronic records.¹² As the PRA and the RTI Act define public records to include ‘any other material produced by a computer’, electronic records are covered within the ambit of the two Acts. However, electronic records require significantly different management techniques than paper records.¹³ For instance, maintenance of electronic records also requires maintenance of proper metadata and data dictionaries, concepts which are altogether absent in the case of paper records.¹⁴ Moreover, unlike paper records, where authenticity of the information is ascertained by

the authority of the paper (say by notarising), in the case of electronic records, the information needs to be treated as separate from the medium where it is being stored, as the medium generally runs the risk of obsolescence due to changes in information technology.¹⁵

As governments are increasingly becoming technology driven, a new development has been taking place in parallel to the discourse on freedom of information and transparency. Open government data, or simply open data movements have been springing up globally, demanding the proactive online release of data and statistics by the governments for public consumption.¹⁶ At the heart of the open data movements is the understanding that governments possess large amounts of data, which, if made public, would stir research and innovation by the private sector and assist in co-producing newer products and services for the public good.¹⁷ Unlike the open government movement which emphasized the civic right to know the workings of the government, the open data movement is targeted at incentivising data scientists, academics, programmers and social entrepreneurs to design solutions to public problems.¹⁸ Open data activists demand for policies and laws which mandate the

11 Kori Schulman, ‘The Digital Transition: How the Presidential Transition Works in the Social Media Age’, (*The White House: President Barack Obama* 31 October 2016) <<https://obamawhitehouse.archives.gov/blog/2016/10/31/digital-transition-how-presidential-transition-works-social-media-age>> accessed 6 December 2020; Rachel Treisman, ‘As President Trump Tweets And Deletes, The Historical Record Takes Shape’, (NPR 25 October 2019) <<https://www.npr.org/2019/10/25/772325133/as-president-trump-tweets-and-deletes-the-historical-record-takes-shape>> accessed 6 December 2020.

12 Section 2(t) and Section 4

13 Sarath Pillai, ‘Old Archival Laws, New Archives’ (2013) Vol. 48, Issue No. 03 *Economic & Political Weekly* <<https://www.epw.in/journal/2013/03/commentary/old-archival-laws-new-archives.html>> accessed 6 December 2020.

14 Luciana Duranti, Terry Eastwood, Heather MacNeil, *Preservation of the Integrity of Electronic Records: 2 (The Archivist’s Library)* (Springer 2002) 14-15.

15 Pillai (n 13).

16 Barbara Ubaldi, ‘Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives’ (2013) 22 *OECD Working Papers on Public Governance* <https://www.oecd-ilibrary.org/governance/open-government-data_5k46bj4f03s7-en> accessed 6 December 2020.

17 *ibid*

18 David E. Pozen & Michael Schudson (eds), *Troubling Transparency: The History and Future of Freedom of Information* (Columbia University Press 2018) 210.

publication of data which is legally, technically and financially open.¹⁹ This means, ideally, open data is government data which is accessible online, machine-readable, redistributable and non proprietary such that it can be processed for future use and application.

Realising the potential of open data and keeping up with the international developments, the National Data Sharing and Accessibility Policy (“NDSAP”) was introduced by the Government of India in 2012.²⁰ The Policy finds its basis in Section 4 of the RTI Act which imposes a duty on public authorities to proactively disclose information to the public.²¹ The NDSAP aims to share all non-sensitive data held by the government agencies which has been generated by using public funds.

In the backdrop of these recent developments in administration and governance, it is of immense importance to examine how the maintenance of these digital records stands the test of transparency and accountability which the legislative framework for public records lays down. What are the strategies and guarantees put in place by the government to check proper delineation and archiving of digital records? To what extent are these safeguards holding strong in practice? Have adequate mechanisms been put in place for the public to access these records and monitor the government in the true spirit of the RTI Act? And finally, is it time to revisit the existing legislations like the RTI Act and the PRA to ensure that they govern these new forms of public records and protect the interests of the citizens? These are some of the questions that this paper attempts to answer.

The paper first explains some of the e-governance initiatives of the Government of India which are the primary sources of digital data and records. It then examines the existing legal framework governing these records to understand their scope and key provisions. On the basis of this, the fourth section of the paper critically evaluates record management practices in India through the lens of access and accountability. In doing so, the paper draws from the experience of the United States of America and makes recommendations for updating the record management laws and policies to ensure they are keeping pace with the changing face of records.

19 Bastiaan van Loenen, Glenn Vancauwenberghe, Joep Crompvoets (eds), *Open Data Exposed* (TMC Asser Press 2018) 3-4.

20 Department of Science & Technology, ‘National Data Sharing and Accessibility Policy’ <<https://dst.gov.in/national-data-sharing-and-accessibility-policy-0>> accessed 6 December 2020.

21 National Data Sharing and Accessibility Policy, 2012 <https://dst.gov.in/sites/default/files/nsdi_gazette_0.pdf> accessed 6 December 2020.

The Transition to E-Governance: Generating e-Records Today

India entered the top 100 countries in the E-Government Index of the United Nations for the first time in 2018.²² However, the Indian government had been advocating for greater technological integration in public functions since long before that. In 2001, the Report of the Working Group on Convergence and E-Governance for the Tenth Five Year Plan (2002-07), released by the Planning Commission, suggested a technology centric process re-engineering for government agencies. Subsequently, e-Governance in India received a major thrust in 2006 under the 11th Five Year Plan (2007-12) wherein Rs. 2942 crores were allocated towards introducing the National e-Governance Plan (“NeGP”).²³ NeGP, in a nutshell, was aimed at providing affordable online services to the citizens and simplifying government processes for increased transparency, efficiency, responsiveness, cost effectiveness and

accountability.²⁴ The NeGP presently includes 44 Mission Mode Projects (MMPs) at three levels, i.e., central, state and integrated projects.²⁵ These collectively cover several key public facing government functions like taxation, immigration, insurance and pensions.

In addition, be it finance and accounting or litigation management, the Central Government has rolled out online platforms for most of its internal administration and all departments are expected to adopt these uniformly. These platforms collect valuable data on government performance and the impact of its decisions. Providing access to this information to citizens is critical for exercising the right to know. Therefore, this section briefly discusses some of the initiatives to highlight the significance of bringing them under the scanner for public accountability in India.

22 UN E-Government Knowledgebase, ‘India’ (2018) <<https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/77-India/dataYear/2018>> accessed 6 December 2020.

23 Planning Commission, Eleventh Five Year Plan (2007–2012), *Inclusive Growth: Volume I*, 230-236 <https://niti.gov.in/planningcommission.gov.in/docs/plans/planrel/fiveyr/11th/11_v1/11th_vol1.pdf> accessed 6 December 2020.

24 National e-Governance Division, ‘Saaransh: A Compendium of Mission Mode Projects under NeGP’ (2011) <[https://www.meity.gov.in/writereaddata/files/Compendium_FINAL_Version_220211\(1\).pdf](https://www.meity.gov.in/writereaddata/files/Compendium_FINAL_Version_220211(1).pdf)> accessed 6 December 2020.

25 National e-Governance Division, ‘Mission Mode Projects’ <<https://negd.gov.in/mission-mode-projects>> accessed 6 December 2020.

A. Administrative Records: E-Office Project

One of the original central projects launched under the NeGP was that of e-Office. Developed by the National Informatics Centre (“NIC”), it is being implemented by the Department of Administrative Reforms and Public Grievances (“DARPG”), Ministry of Personnel, Public Grievances and Pensions. The project aims to ‘achieve a simplified, responsive, effective and transparent working of all government offices’.²⁶ E-office is a product suite comprising 7 services which shift administrative processes like filing, communication, leave management, personnel management and knowledge management to a single ICT enabled platform.²⁷ In the last 5 years its user base has expanded from mere 110 departments in 2014²⁸ to 533 at present.²⁹ This includes 269 Central and 262 State Government departments.

The e-Files system, which is perhaps the most important e-Office service, is intended to enable a paperless office by digitising inward correspondences and creating new files digitally with their respective noting, referencing and correspondence attachment.³⁰ The system is also designed to automatically track the movement of files within and across the departments. E-Office is a break away from the traditional paper based system as it completely dispenses with manual tracking and managing of government files and

correspondences, paving way for a simple process and reducing instances of file mismanagement.

The e-Office website shows that over 1.6 crore electronic files have been created on the system this far.³¹ Even though one of the objectives of the project was to establish transparency and accountability, there is no clear metric to judge whether the platform has met its promise. The aggregated data on its website gives no granularity on the nature, movement or retention of files. Moreover, the compliance of e-files with the PRA and RTI Act is often neglected, as we will see in the later sections of the paper.

B. Financial Records: PFMS and GSTN

In 2008, the Central Government launched the Public Financial Management System (“PFMS”) which is implemented by the Office of Controller General of Accounts. While it was initially used for tracking the funds from the plan schemes of the Centre, its scope has since been widened to cater to all payments of Government of India, as well as all tax and non-Tax receipts. Going forward, it is planned to subsume all other financial software of the Central Government within PFMS³² and extend the platform to State Governments.³³

During the 12th Five Year Plan, the Cabinet approved a total plan outlay of Rs.1080 crore for the national roll out of PFMS over a period

26 E-Office, ‘About Us’ <https://eoffice.gov.in/about_us.php> accessed 6 December 2020.

27 ibid

28 National Informatics Centre, ‘E-Office Book’ (2020) 24 <<https://eoffice.gov.in/downloads/eOfficeBook2020.pdf>> accessed 07 December 2020.

29 E-office, ‘Dashboard’ <<https://eoffice.gov.in/Dashboard/dashboard.php>> accessed 07 December 2020.

30 National Informatics Centre, ‘eOffice: An Implementation Handbook’ (2011) <<http://cwc.gov.in/sites/default/files/admin/005-eOffice-Handbook.pdf>> accessed 07 December 2020.

31 National Informatics Centre, ‘E-Office’ <<https://www.nic.in/projects/e-office/>> accessed 07 December 2020.

32 Controller General of Accounts, ‘PFMS’ <<http://cga.nic.in/Page/PFMS.aspx>> accessed 07 December 2020.

33 Office of Chief Controller of Accounts, ‘PFMS’ <<https://ccaind.nic.in/computerisation.asp>> accessed 07 December 2020.

of 4 years (2013-14 to 2016-17).³⁴ The platform has become a crucial component of major financial transactions. To give context, so far in the Financial Year 2020-21 (approximately 6 months) alone, the PFMS has recorded about 90 crore transactions cumulatively amounting to over Rs 18,000 crores.³⁵ The National Statistical Commission has noted that “The PFMS captures data relating to intergovernmental fiscal transfers, both in terms of payments and receipts, payment of states’ and local bodies’ shares in central taxes, flow of grants of different kinds from any of the public accounts and their utilization by the recipients.”³⁶

The Goods and Services Tax Network (“GSTN”)³⁷ is another digital financial platform which is rich in important information about public transactions. GSTN is a government company and with over 1 crore registered taxpayers, the GSTN performs the public function of gathering data on all transactions involving indirect taxes in the country.³⁸

The PFMS and GSTN can be considered as goldmines of real time granular data on movement of public money. Unfortunately, there have been no attempts whatsoever by the government to share this data publicly. In fact, in response to a query under the RTI Act on

accessibility of the PFMS data, the Department Revenue blankly denied having any plans to make the data public.³⁹ It stated that the data can only be accessed by government employees with their login details, implying thereby that the data is accessible on departmental basis for official use only. By shirking away from its responsibility to publish such financial data, the government not only impinges upon the citizens’ right to information but also impedes the growth and innovation which lie at the heart of open data principles.

C. Legal Records : Legal Information Management & Briefing System

It is well known that the government, as a near compulsive litigant, contributes the largest share of cases in Indian courts. By the estimates of Department of Justice itself, about 46% of the pendency in the courts comes from government litigation.⁴⁰ To streamline the litigation management practices among ministries, the Department of Legal Affairs introduced the Legal Information Management & Briefing System (“LIMBS”) in 2016.⁴¹ LIMBS is an online portal where a nodal officer appointed by each ministry can enter details of a case, the forum, the advocate appointed and the dates of hearings. Advocates

34 Standing Committee on Finance, Ministry of Finance, *Twenty Fourth Report* (16th Lok Sabha, December 2015) <https://eparlib.nic.in/bitstream/123456789/65306/1/16_Finance_24.pdf> accessed 07 December 2020.

35 Public Financial Management System-PFMS, ‘Home’ <<https://pfms.nic.in/NewDefaultHome.asp>> accessed 14 November 2020.

36 National Statistical Commission, ‘Report of the Committee on Fiscal Statistics’ (2018) 68 <<https://mospi.gov.in/documents/213904/0/Report+of+the+Committee+on+Fiscal+Statistics.pdf/51d07475-9c00-9bf6-b6e2-f36420a7f066?t=1595174394877>> accessed 07 December 2020.

37 Goods and Services Tax Network, ‘Home’ <<https://www.gstn.org.in/home>> accessed 07 December 2020.

38 *ibid*

39 Letter no. Dy. No. 1518250/20-Cash dated 12.10.2020 from CPIO, Department of Revenue, Ministry of Finance, Government of India.

40 Department of Justice, ‘Action Plan to Reduce Government Litigation’ (2017) 2 <<https://doj.gov.in/sites/default/files/Government%20litigation%20ppt-June%2012%20revised.pdf>> accessed 07 December 2020.

41 Department of Legal Affairs, Notification No. A-60011/14/2014-Admin.IV(LA) (8 February 2016) <https://www.epfindia.gov.in/site_docs/PDFs/Circulars/Y2017-2018/LC_Registration_LIMBS_5926.pdf> accessed 07 December 2020.

appointed by the government can also set up an account on the portal and update the status of the case for the information of the Ministry.⁴² LIMBS 2.0 also allows for tracking of arbitration matters.

Currently, the user base of LIMBS is spread across 57 Ministries and over 19,000 advocates.⁴³ These users feed into the system valuable data on government litigation which can be used by researchers and the government itself to carry out important analyses and improve not only the litigation management of the governments but also the litigation practice in the country. The data from LIMBS can be an asset for assessing the performance of panel advocates, evaluating the efficiency of the courts from different regions and tracking the compliance records of the government (LIMBS includes a feature to specifically display the contempt cases pending against the department). The government can even use the data to review the costs and benefits involved in the litigation and predict outcomes of the case based on past records.⁴⁴

Despite these possibilities, the government has neither made LIMBS open access nor shared its data with the public.⁴⁵ It may be argued that the veracity of the data is questionable given that, unlike e-Office and PFMS, LIMBS relies on manual entry of data which may be riddled with inaccuracies or incomplete information. Perhaps the Ministry of Law and Justice would be wise to update the application for automatic linking to the e-courts system. Regardless, the information which currently exists on the portal is reflective

of how the government chooses to spend its own and judicial resources and the returns it expects.

Even if these platforms have been successful in bringing efficiency to the government, there is little that they offer in terms of transparency or accountability. In absence of an inbuilt mechanism for sharing information with citizens or enabling access to important documents, a citizen can only hope that the authorities comply with the legal framework that has been put in place for ensuring access. The next section explores the duties imposed on authorities in this regard by the present legislations, policies and guidelines.

42 Department of Legal Affairs, DO Letter No. A-60011/14/2014-Admin.IV(LA) (22 September 2016) <https://www.cbic.gov.in/resources/htdocs-cbec/deptt_offcr/circ-deptl/online-monitrng-court-cases-limbs-portal-1.pdf> accessed 07 December 2020.

43 Legal Information & Management Briefing System (LIMBS) <<https://limbs.gov.in/limbs/>> accessed 15 November 2020.

44 Bibek Debroy, 'A Justice More Efficient' (*The Indian Express*, 14 June 2018) <<https://indianexpress.com/article/opinion/columns/legal-information-management-and-briefing-system-limbs-government-litigation-5216317/>> accessed 07 December 2020.

45 *ibid*

Legal Framework for Governance of e-Records and Data

The switch from the physical to the digital medium in public functions begs the questions: What is the legal framework for managing such a large volume of electronic records and accessing data in India? And more importantly, is the government being checked for its duty to be accessible and open? This section seeks to answer these questions with the intention of analysing whether the online platforms meet the standards of transparency and accountability which the law imposes. First, a brief introduction of the two primary legislations governing records management and access, i.e., PRA and RTI Act has been provided. Thereafter, described in brief are executive policies, standards and guidelines pertaining specifically to electronic records.

A. The Public Records Act and the Right to Information Act

The PRA was enacted in 1993, to regulate the management, administration and preservation of public records of the Central Government and Union Territory Administrations. At the time of its tabling in the Lok Sabha, it was observed that such a uniform law was critical for making ‘records easily accessible to research scholars and also facilitate quick transfer of records of permanent value to the Archives.’⁴⁶ The Act mandates every authority under the Central Government to nominate a records officer who shall be responsible for all record management activities of the authority including periodic reviews, compilation of indices and transferring public records to the National Archives of India (“NAI”). These central agencies are also required to prepare records retention schedules for the periodic weeding and preservation of their

46 Eighth Session, Tenth Lok Sabha, *Lok Sabha Debates* (Volume XXVI No. 6, 1993) <https://eparlib.nic.in/bitstream/123456789/3249/1/lsd_10_8th_09-12-1993.pdf> accessed 07 December 2020.

records. Several states like Bihar,⁴⁷ Karnataka,⁴⁸ Himachal Pradesh⁴⁹ and Maharashtra⁵⁰ have also enacted their own public records legislations to govern their internal administration.

The RTI Act is a powerful legislation for exercising the fundamental right to information. Under the Act, a citizen merely has to file an application, in no particular format, with the Public Information Officer (“PIO”) of a public authority, and the PIO is bound to share the information within 30 days. In their application, citizens are not required to submit proof of their identity nor disclose the purpose for seeking the information. The grounds on which information can be denied have been limited in the Act and failure to provide information on any other ground would invite a penalty on the concerned PIO.

Despite the noble intentions behind the two legislations, the obstinate suspicion of the Indian bureaucracy towards transparency and public enquiries has brought their actual implementation and impact under question. Further, the mechanisms stipulated for accessing information under the Acts can prove to be practically inconsistent. These aspects are discussed in more detail in the next chapter.

B. CSMOP & CSeMOP

The specific guidance on electronic records management is primarily contained in the Central Secretariat Manual of Procedure (“CSMOP”) which is released by the DARPG.⁵¹ The Manual lays down the procedure for file management including instructions on file noting, numbering and retention for both - physical and e-files. Additionally, the DARPG has also released the Central Secretariat Manual of e-Office Procedure (“CSMeOP”) in 2012 for the purpose of implementing the e-Office project.⁵² The Manuals collectively provide the following salient procedures for governing e-files:

1. For each new e-file, a unique file number will be generated automatically.
2. The movement of e-files from one department to another will be automatically tracked.⁵³ This will include date and time of transfer and details of the sender and the recipient.
3. The gist of important files will be disclosed on the website of the department, in compliance with RTI Act, before the e-file is recorded for closing.
4. Records will be split into Category I (permanent records of historic value) and Category II (of secondary importance having reference value of not more than 20 years).⁵⁴ Category I files are sent to the NAI for long term preservation.

47 The Bihar State Public Records Act, 2014 <https://prsindia.org/files/bills_acts/acts_states/bihar/2014/2014Bihar8.pdf> accessed 07 December 2020.

48 Karnataka State Public Records Act, 2010 <<https://www.latestlaws.com/bare-acts/state-acts-rules/karnataka-state-laws/karnataka-state-public-records-act-2010/>> accessed 07 December 2020.

49 The Himachal Pradesh Public Records Act, 2006 <https://hprural.nic.in/HP_%20Act2006.pdf> accessed 07 December 2020.

50 The Maharashtra Public Records Act, 2005 <<http://www.bareactslive.com/MAH/MH214.HTM>> accessed 07 December 2020.

51 Department of Administrative Reforms and Public Grievances, ‘Central Secretariat Manual of Office Procedure’ (14th Edition, 2015) <https://darpg.gov.in/sites/default/files/CSMOP_0_0.pdf> accessed 07 December 2020.

52 Department of Administrative Reforms and Public Grievances, ‘Central Secretariat Manual of e-Office Procedure’ (1st Edition, 2012) https://darpg.gov.in/sites/default/files/CSMeOP_1st_Edition.pdf

53 CSMeOP (n 52) 57-58.

54 Ibid 59.

5. Back up of digital records is to be taken periodically. One copy will remain in the Digital Record Room created in the e-Office and a second copy will be stored at Disaster Recovery Site to be maintained by NIC/NAI.⁵⁵

Since the e-file system in the e-Office suite has been designed by the NIC to be in compliance of these requirements,⁵⁶ it could usher in greater efficiency, transparency and accountability in the government departments. Its functionalities like an e-signature feature (linked to the Aadhaar number of the officer) and automatic updation of concerned employees in the File Tracking System during internal movements of files,⁵⁷ could significantly curb malpractices in the Indian bureaucracy such as hiding or destroying part or whole files, which is unfortunately a common practice in the paper based system. The automated numbering and tracking, and auto generated reports detailing the employees associated with the file could help to hold individuals accountable for their actions. All of this is of course subject to the rigorous implementation of the e-Office and an absolute transition from the paper files.

C. E-governance standards

The long term preservation of these e-files has not escaped the government's agenda. In accordance with the recommendations of the National Study Report on Digital Preservation Requirements of India,⁵⁸ MeitY has notified⁵⁹ two Digital Preservation Standards which are applicable to those electronic records which are to be preserved either long term or permanently:

1. [Best Practices & Guidelines for Production of Preservable e-Records \(PRoPeR\), 2013](#)⁶⁰ - The guidelines identify the key characteristics of preservable electronic records and recommend preferable storage formats. They lay down a five staged e-records management procedure.
2. [e-Governance Standard for Preservation Information Documentation \(eGOV-PID\) of Electronic Records, 2013](#)⁶¹ - These standards are targeted at ensuring that electronic records adopt a standardized metadata dictionary and schema.

⁵⁵ Ibid 62.

⁵⁶ National Informatics Centre, 'File Management System: User Manuel' (2018) 7 <<https://docs.eoffice.gov.in/eFileMU.pdf>> accessed 08 December 2020.

⁵⁷ ibid

⁵⁸ 'National Report on Digital Preservation Requirements of India: Volume 1' (C-DAC 2011) 12 <http://www.ndpp.in/download/study_report/Volume-1-DPS-Report-ISBN-978-81-909383-1-0.pdf> accessed 08 December 2020.

⁵⁹ Department of Electronics and Information Technology, Notification, (13 December 2013) <<http://www.ndpp.in/download/standard/Notification-Digital-Preservation-Standard.pdf>> accessed 08 December 2020.

⁶⁰ Department of Electronics and Information Technology, 'Best Practices & Guidelines for Production of Preservable e-Records (PRoPeR), 2013' <<http://egovstandards.gov.in/sites/default/files/Best%20Practices%20and%20Guidelines%20for%20Production%20of%20Preservable%20e-Records%20Ver1.0.pdf>> accessed 08 December 2020.

⁶¹ Department of Electronics and Information Technology, 'e-Governance Standard for Preservation Information Documentation (eGOV-PID) of Electronic Records, 2013' <<http://egovstandards.gov.in/sites/default/files/e-Governance%20Standards%20for%20Preservation%20Information%20Documentation%20of%20e-Records%20Ver1.0%20%28Metadata%20%26%20Schema%29.pdf>> accessed 08 December 2020.

D. National Data Sharing and Accessibility Policy

The NDSAP of 2012 draws from the RTI Act and lays a foundation for democratising access to the data which has been built and collected using the taxpayers' money.⁶² The release of this data in the public domain was expected to minimise individual applications under the RTI Act which are relatively more time and cost intensive. By requiring all Central ministries and departments to publish all shareable data in a machine readable format and clearly identify the 'negative list' of non shareable data, the Policy also aims to facilitate private use of this information for research and innovation. To this end, Open Government Data ("OGD") Platform of India (data.gov.in) is supposed to serve as the single unified source for all quality government data in open formats with all the associated metadata.

Interestingly, the Platform has been designed to automatically fetch data from eGov applications by discovering the metadata should the relevant Department choose to share it.⁶³ In order to prompt the Departments to comply, the implementation guidelines of the Policy create

a structure involving a Chief Data Officer and an NDSAP cell at each Department who shall be responsible for identifying and sharing datasets. Besides the Centre, 12 states⁶⁴ have adopted the NDSAP while five states, namely, Sikkim, Tamil Nadu, Odisha, Punjab and Kerala have set up their own sub-domains on the OGD Platforms.

Moreover, MeitY had also introduced the Policy on Open Application Programming Interfaces for Government of India ("Open API Policy") in 2015 to promote interoperability of the government softwares to enable private access.⁶⁵ This too has been incorporated in the OGD Platform which currently gives access to over 64,000 APIs.⁶⁶

The NDSAP adopts a positive approach where it encourages the government to share its data. As a policy, it does not subscribe to the negative language of sanctions, because of which the bureaucracy is not usually on the back foot with regards to the NDSAP as is often the case with the RTI Act. Scholars have also touted the open data route as the 'new low-hanging fruit of good governance'.⁶⁷ It comes as no surprise then that several expert committees and ministry reports have endorsed the implementation of the

62 National Data Sharing and Accessibility Policy 2012 <<https://data.gov.in/sites/default/files/NDSAP.pdf>> accessed 08 December 2020.

63 National Informatics Centre, 'Implementation Guidelines for National Data Sharing and Accessibility Policy (NDSAP)' (Ver. 2.4, 2015) 15 <<https://data.gov.in/sites/default/files/NDSAP%20Implementation%20Guidelines%202.4.pdf>> accessed 08 December 2020.

64 Tamil Nadu, Punjab, Madhya Pradesh, Sikkim, Haryana, Kerala, Meghalaya, Gujarat, Odisha, Chhattisgarh, Delhi and Karnataka. Source: Letter no. F.No. 17/2/2019-NSDI dated 25.11.2020 from CPIO, NSDI received in response to an RTI Application filed by the author.

65 Department of Electronics and Information Technology, 'Policy on Open Application Programming Interfaces (APIs) for Government of India' (2015) <https://www.meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf> accessed 08 December 2020.

66 Open Government Data (OGD) Platform India, 'API' <<https://data.gov.in/ogpl/apis>> accessed 17 November 2020.

67 Sumandro Chattapadhyay, 'Towards an Expanded and Integrated Open Government Data Agenda for India' (*Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance*, 2013) <https://github.com/hasgeek/oddc/blob/master/docs/sumandro_expanded_and_integrated_ogd_agenda_for_india.md> accessed 08 December 2020.

NDSAP.⁶⁸ However, this non-adversarial tone of the Policy is perhaps more a bane than a boon, as shall be discussed in the next chapter.

E. Policies and Guidelines Governing Electronic Communications (Emails, social media and websites)

Much of government's internal and external communication now takes place online. As per official figures,⁶⁹ there are over 2.6 lakhs official government email accounts which see a daily traffic of 2.5 crore emails on an average. The average monthly traffic for SMS from government applications is a whopping 112 crores. The actual number of emails and messages serving official business is likely to be much higher as several officials continue to use private services. The NIC is also in the process of developing an Instant Messaging System on the lines of WhatsApp for the internal use of the government.⁷⁰ Moreover, the government relies extensively on social media for communicating real time updates directly to the masses.⁷¹

Even though emails have been around for a while, the government did not introduce any regulatory mechanism for their agencies for the longest time. In 2012, a PIL was filed in the Delhi High Court by K.N. Govindacharya questioning the use of private services like Gmail and Yahoo mail for official purposes. He contended that since government emails constitute official public records, the use of private channels with overseas servers is a violation of the Public PRA.⁷² The Delhi High Court accepted this contention and directed the Central Government to expeditiously formulate an email policy which complies with the requirements of the PRA.⁷³

Subsequently, in 2014, MeitY notified the E-mail Policy of Government of India⁷⁴ along with its supporting guidelines.⁷⁵ NIC is the implementation body for the Policy and only the email services of NIC can be used for all official communications of the Central Government. State departments which use the email service of NIC are also bound by the Policy. Rather than tracing its roots to the PRA, the Policy is claimed to be an extension of the CSMeOP. It prohibits downloading or transferring official

-
- 68 Department of Economic Affairs, 'Report of the Steering Committee on Fintech Related Issues' (2019) 136-137 <https://dea.gov.in/sites/default/files/Report%20of%20the%20Steering%20Committee%20on%20Fintech_2.pdf> accessed 08 December 2020; National Statistical Commission (n 36); Ministry of Electronics and Information Technology, 'Report by the Committee of Experts on Non-Personal Data Governance Framework' (2020) 65 <https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf> accessed 08 December 2020.
- 69 Standing Committee on Information Technology, Ministry Of Electronics And Information Technology, *Demands For Grants (2019-20), Fourth Report*, (17th Lok Sabha, December 2019) 10 <http://164.100.47.193/lssccommittee/Information%20Technology/17_Information_Technology_4.pdf> accessed 08 December 2020.
- 70 Ibid 49.
- 71 Kiran Subbaraman, 'Governments' Love-Hate Relationship with Social Media' (*Forbes India*, 13 March 2013) <<https://www.forbesindia.com/blog/technology/governments-love-hate-relationship-with-social-media/>> accessed 08 December 2020.
- 72 Press Trust of India, 'Frame email policy for officials within a month: HC to govt' (*Business Standard*, 30 October 2013) <https://www.business-standard.com/article/politics/frame-email-policy-for-officials-within-a-month-hc-to-govt-113103000806_1.html> accessed 08 December 2020.
- 73 High Court of Delhi, W.P.(C) 3672/2012 and CM Nos.7709/2012, 12197/2012 and 6888/2013, Order dated 30.10.2013 <http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=211444&yr=2013> accessed 08 December 2020.
- 74 Department of Electronics and Information Technology, 'E-mail Policy Of Government of India' (2014) <https://www.meity.gov.in/writereaddata/files/E-mail_policy_of_Government_of_India_3.pdf> accessed 08 December 2020.
- 75 Department of Electronics and Information Technology, 'Guidelines for E-mail Account Management and Effective E-mail Usage' (2014) <https://www.meity.gov.in/writereaddata/files/Guidelines%20for%20E-mail%20Account%20Management%20and%20Effective%20E-mail%20Usage_0.pdf> accessed 08 December 2020.

emails on private accounts and recommends that sensitive emails should be encrypted or certified with digital signature. The mechanism for data retention has been left to be decided by each individual agency while the NIC is supposed to take backup of emails on a regular basis. States like Haryana,⁷⁶ Madhya Pradesh⁷⁷ and Telangana⁷⁸ have also introduced similar policies for their respective governments.

Additionally, DeitY has released the 'Framework & Guidelines for Use of Social Media for Government Organisations' in 2012⁷⁹ which give guidance to government departments on utilizing social media for optimal engagement with the citizens. In terms of records retention, the guidelines specifically require all necessary records and trails to be maintained by the department in cases where consultations which are likely to influence policy outcomes are undertaken on social media platforms. Moreover, the document acknowledges that most social media platforms are owned and operated overseas and thus specific regulations and Service Level Agreements are necessary for ensuring storage and archival of information within India.

For governing websites, DARPG has issued the 'Guidelines for Government Websites' as an extension of the CSMOP.⁸⁰ The guidelines issue directions for website designs and content sharing in an accessible manner. Specifically, all documents which are uploaded on the website

should display the date of the document so that they can be removed and archived offline as necessary.

Surprisingly, much like the Email Policy, neither the Social Media Framework nor the website guidelines makes any reference to the PRA. While both take into consideration concerns of access and compliance with the RTI Act, they end up giving a lot of leeway to individual departments to evolve their own practices. It appears like DARPG and MeitY, in their best intentions to develop standards competent with the world, have perhaps unwittingly ignored the provisions of the Indian law. More detailed discussion on this aspect is undertaken in the coming chapter.

76 Letter No. 3/28/2000/3SIT/3693 dated 15.07.2016 from Principal Secretary to Government Haryana, Electronics &, Information Technology Department <<https://cdnbbsr.s3waas.gov.in/s35352696a9ca3397beb79f116f3a33991/uploads/2020/07/2020071447.pdf>> accessed 08 December 2020.

77 Madhya Pradesh Government Email Policy 2014 <<https://harda.nic.in/en/document/mp-government-email-policy/>> accessed 08 December 2020.

78 Email Policy of Government of Telangana 2016 <https://www.it.telangana.gov.in/wp-content/uploads/2016/07/20012016ITC_MS2.pdf> accessed 08 December 2020.

79 Department of Electronics and Information Technology, 'Framework & Guidelines for Use of Social Media for Government Organisations' (2012) <https://www.meity.gov.in/writereaddata/files/Approved%20Social%20Media%20Framework%20and%20Guidelines%20_2_.pdf> accessed 08 December 2020.

80 Department of Administrative Reforms and Public Grievances, 'Guidelines For Indian Government Websites' (2018) <https://darpg.gov.in/sites/default/files/gigw-manual_Revised2018.pdf> accessed 08 December 2020.

Shortcomings in Effective e-Records Management

The above described legal framework, though well intended, seems to be falling short in achieving its mandate. This chapter highlights the several drafting and implementation shortcomings which are rendering ineffective the e-records and data management regimes in the country.

A. Inconsistencies between the legal framework

The PRA and the RTI Act were brought into force with a difference of 12 years between them. This period, fuelled by technology, witnessed a paradigm shift in the governance framework in India. While the RTI Act has imbibed this understanding of governance in its provisions, the PRA has never been amended to adapt to the changing times. Below are three aspects which highlight the conceptual inconsistencies between the RTI Act, the PRA as well as the executive policies and the practical implications these have

for the accessibility and accountability framework in India in the current times.

Scope of application

The RTI Act covers public authorities both at the central and the state level. However, the PRA is confined to central record creating agencies in its scope. There is arguably also a finer distinction between the scope of application of the Acts. The RTI Act takes a broader approach and covers bodies owned, controlled or substantially financed by the government.⁸¹ It also includes non-governmental organisations which are substantially financed by the government. On the contrary, the PRA takes a narrower approach by extending to only statutory bodies or corporations wholly or substantially controlled or financed by the government.⁸² Thus records of those private organisations that might be performing a public function or are being financed substantially by public money are not technically considered as public records under the PRA and thus are not required to be preserved in compliance with the Act. This should be considered a grave omission

⁸¹ Section 2(h)

⁸² Section 2(f)

as the government is moving increasingly towards privatisation of public functions which have direct implications for the citizens at large.⁸³

Procedure for access

The two legislations also prescribe very different regimes for accessing documents. The strength of the RTI Act lies in the simplicity with which a citizen can request for information from the public authority. The Act gives very little room to the PIO to wiggle out of sharing the requested information, with the only exception being carved out under the straightjacket exemptions listed in Section 8 of the Act. On the other hand, the procedure for accessing archives stored at the NAI is fairly restrictive on multiple counts. First, the Public Records Rules, 1997 allow access to the national archives only for 'bona fide consultation and research purpose'⁸⁴ Second, the archives are made accessible only to research scholars and the mandatory Form A that needs to be filed to gain access has a mandatory requirement of attaching a letter of recommendation from the university with which the researcher is affiliated. Third, the Director General or the Head of Archives under Rule 11 enjoys the discretion to reject the application to access archives. The rules do not mention the grounds on which this rejection can be made but only require that the reason for rejecting the application be recorded in writing.

Timelines

Across the two legislations as well as the guidelines and policies released by DARPG and MeitY, there is a stark discrepancy as to the time period beyond which the relevant documents need to be archived and made accessible to the public.

As regards preservation, the Email Policy of Government of India authorizes NIC to delete all email logs after two years irrespective of their content, which is blatantly against the PRA. The CSMeOP in para 94 requires Category-I e-files, that is, e-files of historic importance which need to be preserved, to be transferred to the NAI after 20 years of coming into existence. Contrary to this, the transfer of permanent records needs to be conducted after 25 years under the PRA. The author contacted the NAI for clarity on the timeline being followed in practice and was informed that electronic records shall be transferred to the NAI on completing 20 years. Therefore, practically, the provisions of an executive Manual are currently superseding the provisions of a legislation. This is technically not sound in law, making it a prime example of why the PRA needs to be updated.

PRA and the RTI Act also provide inconsistent schedules for access. Under the former, a person can only access the records from the NAI which are 30 years old. As opposed to this, the RTI mechanism puts no bar on time of access and a citizen can request for a document from any period of time. This in effect makes the provision of 30 years under the PRA redundant as a citizen can file an application with the NAI for any document which has not yet completed 30 years of existence. Therefore, the law needs to be revised to harmonize these differences.

B. Lacunae in the PRA

As mentioned earlier, the PRA has not been amended since it was enacted in 1993 despite the changes in the discourse of governance and

⁸³ Alok Prasad, 'Two Decades Of Public Records Act (1993): A Critical Re-Appraisal' (*Proceedings of the Indian History Congress*, vol. 74, 2013) 1025–1033 <www.jstor.org/stable/44158909> accessed 8 December 2020.

⁸⁴ Rule 11

transparency which have ensued since then. Consequently, it adopts an understanding of records and access which are not in tandem with the demand and sensitivities of the contemporary India.

The PRA and RTI Act⁸⁵ both define records in terms of the medium in which information is stored, i.e., (a) any document, manuscript and file; (b) any microfilm, microfiche and facsimile copy of a document; (c) any reproduction of image or images embodied in such microfilm (whether enlarged or not); and (d) any other material produced by a computer or any other device. This understanding of record is restricted to capturing the records stored in the form of traditional paper files and born-digital computer files. However, as the government engages with technology in newer, more sophisticated ways, this medium-centric definition fails to encapsulate in essence the varied forms of records being generated in the process – e.g. data captured through government applications and the metadata associated with e-files. It also offers no safeguard against the risk of obsolescence of digital formats.

The Federal Records Act, 1950 of the United States of America, which is quite similar to the Public Records Act of India in its purpose and structure, originally adopted a similar definition of records. However, in 2014, the definition was amended by the Presidential and Federal Records Acts Amendment to “*shift the emphasis away from the physical media used to store information to the actual information being stored, regardless of form*

or characteristic.”⁸⁶ Therefore, the new position of law in the US is that all recorded information that pertains to the performance of a Federal function or other activities of the Government is governed by the Federal Records Act and is accessible under the Freedom of Information Act, format no bar. As a result, a larger volume of information is now expected to be transferred to the National Archives and Records Administration (“NARA”) (American counterpart of the National Archives of India) by the government.

In terms of access, as already mentioned, the PRA was enacted with research scholars in mind as the targeted beneficiaries. Therefore, it allows access to only researchers who can show an academic affiliation. With the acceptance of the right to information as a fundamental right, it is high time that the PRA be amended to afford access to the records archived at NAI to any citizen. Such an attempt was made in 2014 when a Public Records (Amendment) Bill⁸⁷ was floated in the Lok Sabha. The Bill proposed the introduction of “electronic records” in the definition of “public records” and the replacement of the words “research scholar” with the word “public”. However, this proved to be of no avail.

Amending the PRA to govern the contemporary records is critical to ensure that information of national and local importance is not lost over time.⁸⁸ The US is now speculating the possibility that President Trump will wipe out official records before leaving office and take advantage of the discretion afforded under the Presidential

85 Section 2(e) of PRA Section 2(i) of RTI Act.

86 Wendy Ginsberg, ‘Common Questions About Federal Records and Related Agency Requirements’ (*Congressional Research Service*, 2015) <<https://fas.org/sgp/crs/secrecy/R43072.pdf>> accessed 08 December 2020.

87 The Public Records (Amendment) Bill, 2014 (Bill No. 180 of 2014) <<http://164.100.24.219/billtexts/lbills/lbills/AsIntroduced/3228LS.pdf>> accessed 09 December 2020.

88 C-DAC (n 58) 22.

Records Act as regards its enforcement.⁸⁹ India needs to draw lessons from this experience in order to ensure its affairs are recorded for posterity and put the updating of the PRA on its agenda. Else, there will be little left to look back and learn from in the future.

C. Limitations of the Open Data Policy

Much like several other laws and policies, the NDSAP successfully establishes a new structure with new posts and offices. However, it lacks foresight in design on several counts for a deeper impact.

First, as a mere policy, it lacks the teeth for enforceability. It is therefore no surprise that several ministries having generous volumes of data are defying the Policy and keeping their datasets confidential.⁹⁰ The initiatives of the government such as the PFMS and LIMBS which gather crucial information find no reflection on the OGD Platform, despite the metadata discovery feature which can automatically fetch data if enabled on the application. This is particularly disturbing given the fact that most of these operations are already running digitally and opening this data would prove to be no hard task for the government. In fact, on perusal of the datasets from Ministry of Finance and Ministry of Law and Justice, it becomes clear that the datasets have not been updated in years. Therefore, essentially the resource base of over 9 thousand catalogs which the Platform flaunts, often contains incomplete or outdated data which is of

very little practical use.⁹¹ Members of the open data community suspect that the apathy stems from lack of awareness as regards the existence of the Policy.⁹²

Second, while the implementation guidelines lay emphasis on quality, accessibility and usability, they fail to define the contours of these terms. As a result, merely dumping aggregated statistics as opposed to granular data is sufficient to show compliance with the Policy. Similarly, the question of accessibility of data in regional languages finds no mention in the Policy or its Implementation Guidelines.

Third, the problem of incapacity plagues the NDSAP. The post of Chief Data Officers remains vacant for several departments and many of those who fill the position are not sensitized to good open data practices. For instance, on the OGD platform itself, out of the 106 listed posts of Chief Data Officers in Central Ministries, 53 have been identified as 'Awaiting new nomination'.

The Policy is not being widely used despite its many advantages. The situation is worse in the case of states as only few states have signed up to open their data. For researchers and entrepreneurs it is often this ground level information which is valuable for meaningful analysis and development of useful applications. From a governance perspective, access to this data is important not only for accountability purposes, but also for policy actors to engage in more informed policy debates.

89 'Politico: Biden may have trouble unearthing Trump's national security secrets' (*Government Accountability Project*, 10 November 2020) <<https://whistleblower.org/in-the-news/politico-biden-may-have-trouble-unearting-trumps-national-security-secrets/>> accessed 08 December 2020.

90 Thejesh G N, 'Open Data in India: In a Restrictive Copyright Regime, Voluntary Organisations Pitch in to Make Data Accessible' (2020) (Vol. 55, Issue No. 23, Economic & Political Weekly) <<https://www.epw.in/engage/article/voluntary-organisations-india-counteract-states-copyright-regime-open-data>> accessed 08 December 2020.

91 Ibid

92 Interview with members of an organisation working in data analysis for civic engagement.

The US experienced a similar difficulty in implementing its Open Data Policy of 2013. The directives issued by the Obama Administration under the policy had limited effect due to reasons such as duplication of platforms for sharing information, dumping raw information which was not machine readable and using proprietary formats for the data.⁹³ Consequently, the Open, Public, Electronic and Necessary (OPEN) Government Data Act, 2019⁹⁴ has been enacted to impose a legal obligation on all federal agencies for sharing all non-sensitive federal data in conformance to the open data principles. The Act, in practice, supplements earlier laws like the Digital Accountability and Transparency Act (DATA) Act, 2014 which requires full disclosure of Federal expenditures for the review and use of taxpayers and policy makers.⁹⁵

In India too, one way to crystallise the open data ethos further can be lending legislative backing to the Policy. As mentioned earlier, the NDSAP traces its origins to Section 4 of the RTI Act which mandates all public authorities to proactive publish all necessary information through means such as the internet to maximise access to the public and minimise individual applications for information under the Act. Perhaps it can be considered to harmonise the RTI Act and the NDSAP by making it explicitly clear under the Act that the disclosures need to be reflected on the centralised platform in open formats.⁹⁶ This would strengthen both, the proactive disclosure

requirement under the Act as well as the principles under the NDSAP.

D. Failure to preserve electronic communications

Managements of records generated through online communications in the form of emails, SMS and social media posts is perhaps the most neglected aspect of electronic public records management in India. A good example of this is the fact that, in contravention to the Email Policy, several government agents continue to prefer email services of international private companies with overseas servers over the NIC services.⁹⁷ Moreover, since several state departments do not use NIC services, they are not covered under the Policy and are thus not obligated to conform to its terms.

Having said so, the Email Policy as well as the social media and website guidelines are in themselves not comprehensive documents. For instance, the question of deciding confidentiality of content has been largely left to the whims of the user agency. There is no prescribed standard on what would constitute confidential or non shareable information. It can be argued that this ambiguity even creates room for denying information under the RTI Act.⁹⁸ In fact, in para 9 titled 'Scrutiny of emails/Release of logs', the Email Policy states the following:

⁹³ United States Senate, 'Report Of The Committee On Homeland Security And Governmental Affairs' (Senate Report 115-134) <<https://www.govinfo.gov/content/pkg/CRPT-115srpt134/html/CRPT-115srpt134.htm>> accessed 08 December 2020.

⁹⁴ Hyon Kim, 'Data.gov at Ten and the OPEN Government Data Act' (Meta - The Data.Gov Blog, 2019) <<https://www.data.gov/meta/data-gov-at-ten-and-the-open-government-data-act/>> accessed 08 December 2020.

⁹⁵ Tasha Austin et al., 'Future of Open Data: Maximizing the Impact of the OPEN Government Data Act' (Data Foundation, 2019) <<https://www.datafoundation.org/future-of-open-data-maximizing-the-impact-of-the-open-government-data-act>> accessed 08 December 2020.

⁹⁶ Chattapadhyay (n 67).

⁹⁷ Standing Committee on Information Technology (n 69) 49.

⁹⁸ Venkatesh Nayak, 'New e-mail policy announced by the Government of India' (RTI Foundation of India, 28 February 2015) <<http://www.rtifoundationofindia.com/new-e-mail-policy-announced-government-india#.X7T-AWgzBIU>> accessed 08 December 2020.

“9.1 Notwithstanding anything in the clauses above, the disclosure of logs/e-mails to law enforcement agencies and other organizations by the IA would be done only as per the IT Act 2000 and other applicable laws

9.2 The IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny of e-mails or release of logs.

9.3 IA will maintain logs for a period of two years.”

Para 9.2 is blatantly in violation of the RTI Act while the blanket destruction on under 9.3 is a direct contravention of the PRA.

A more serious issue however is the absolute absence of provisions on compliance with the PRA across the three documents. There is no mention of the fact that these records must be retained within the confines of the PRA and cannot be circulated or destroyed in contravention to the Act.

Once again, by and large the user department is given almost unbridled freedom to decide on the course of action for data retention and archival.

Regardless of this omission, the legal position is clear that the PRA applies to all communications of the government which are made in the official capacity even if they are produced from a computer. Any policy or guideline which is framed by the executive must be applied only in consonance with the law passed by the

legislature. The Delhi High Court was cognizant of this in its orders while deciding the PIL filed by K.N. Govindacharya where it directed that the email policy should be drafted keeping in view the safeguards prescribed under the PRA. In fact, under the pressure from the Court, DeitY released two office memorandums in 2014, advising departments to comply with the PRA while using government email ids and social media accounts.⁹⁹ However, in a country where the existence of PRA is not known to several officials, mere office memorandums are unlikely to have much impact. Making an unequivocal reference to the PRA in all the intra-government policies and guidelines for the three primary media of communication intra is the least that the Departments could do while drafting these documents.

A more comprehensive framework for governing the electronic communications in India is important for avoiding what was experienced with Secretary of the State Hillary Clinton in the US. Clinton was found to have been using her private email id linked to her private server for conducting official correspondence, instead of the government authorised email account.¹⁰⁰ By doing so, she gained unchecked control over retention and destruction of critical government information. In the wake of this controversy, the Obama administration enacted the Presidential and Federal Records Act Amendments of 2014 which prohibits the use of private email accounts unless the email is copied to or forwarded to an official email account within 20 days of its creation.¹⁰¹

⁹⁹ High Court of Delhi, W.P.(C) 3672/2012 and CM APPL Nos. 7709/2012, 12197/2012, 6888/2013 and 5628/2014, Order dated 28.11.2014 <http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=241357&yr=2014> accessed 08 December 2020.

¹⁰⁰ Anthony Zurcher, ‘Hillary Clinton emails - what’s it all about?’ (BBC, 6 November 2016) <<https://www.bbc.com/news/world-us-canada-31806907>> accessed 08 December 2020.

¹⁰¹ Presidential And Federal Records Act Amendments Of 2014 <<https://fas.org/sgp/congress/2014/pr.html>> accessed 08 December 2020.

The use of social media by the President of the US is posing a similar challenge for the US. Barack Obama joined Twitter in his official capacity as the President and President Trump inherited the account on his departure. But while the former used an automated system for archiving his social media content, the latter is raising concerns over violation of Presidential Records Act by deleting his tweets.¹⁰²

Broadly worded policies, such as those which currently exist in India, are not sufficient for ensuring good recordkeeping practices within the government. Giving these a legislative backing is imperative and for this purpose amending the PRA to enlarge its scope is the perhaps the first step. In the larger picture, the PRA and RTI Act need

¹⁰² Treisman (n 11).

Conclusion

The above discussion on electronic records management in India makes two things abundantly clear – first, the electronic records and data in the country are largely being governed by executive policies and guidelines. Second, the two legislations which do apply to electronic records are not comprehensive enough to cater to the changing face of records in the country. The Standing Committee on Information Technology had way back in 2005 noted *that the age old statutes and regulations governing the manual process will not be suitable for governing the electronic processes which require altogether a different set of legal framework and guidelines to make the e-Governance successful.*¹⁰³ In 2008, the Second Administrative Reforms Commission had similarly noted that the scope of the NeGP was too large to be governed effectively by the IT Act.¹⁰⁴ Therefore, it recommended the formulation of a new legal framework for e-governance to optimise coordination between

the government agencies and establish adequate monitoring and implementation mechanisms.

While this was observed in the context of process reengineering, it also holds true specifically for records management. The present legal framework for electronic records only scrapes the surface when it comes to addressing the real issues affecting the e-records management. The PRA and the RTI Act in particular need to be revisited in the backdrop of the recent developments in technology and governance. At the same time the executive needs to review its guidelines and policies to make them more comprehensive and aligned with the law of the land.

Formalising the procedure for electronic records management is only the first, albeit the most important, step towards ensuring their access and attributing accountability. To really drive the transparency wave in the country, what is

¹⁰³ Standing Committee On Information Technology (2005-2006), *Implementation Of E-Governance Projects Twenty-Second Report* (14th Lok Sabha, December 2005) <https://eparlib.nic.in/bitstream/123456789/62991/1/14_Information_Technology_22.pdf#search=null%2014%202005> accessed 08 December 2020.

¹⁰⁴ Second Administrative Reforms Commission, 'Eleventh Report - Promoting e-Governance: The SMART Way Forward' (2008) <https://darp.gov.in/sites/default/files/promoting_egov11.pdf> accessed 08 December 2020.s

truly needed is political will. It is only when the bureaucracy becomes conscious of its duty to the public can there be meaningful civic participation and enhanced efficiency in the system. And this consciousness can be stirred only by citizens who endeavour to keep the conversation alive by asking the right questions and nudging the government to be more open. The scholars, historians, researchers, innovators and civil societies need to continuously push for exercising their rights. Building information rich archives and resources is essential for progressing towards a future which progressively learns from the present.

