Privacy Gaps in India's Digital India Project

AUTHOR **Anisha Gupta**
EDITOR **Amber Sinha**

The Centre for Internet and Society, India

Designed by **Saumyaa Naidu**

Introduction

The Central and State governments in India have been increasingly taking steps to fulfill the goal of a 'Digital India' by undertaking e-governance schemes. Numerous schemes have been introduced to digitize sectors such as agriculture, health, insurance, education, banking, police enforcement, etc. With the introduction of the e-Kranti program under the National e-Governance Plan, we have witnessed the introduction of forty four Mission Mode Projects.[1] The digitization process is aimed at reducing the human handling of personal data and enhancing the decision making functions of the government. These schemes are postulated to make digital infrastructure available to every citizen, provide on demand governance and services and digital empowerment.[2] In every scheme, personal information of citizens are collected in order to avail their welfare benefits. While the efforts of the government are commendable, the efficacy of these programs in the absence of sufficient infrastructure for security raises various concerns. Increased awareness among citizens and stronger security measures by the governments are necessary to combat the cogent threats to data privacy arising out of the increasing rate of cyberattacks.[3]

Scope

This paper seeks to assess the privacy protections under fifteen e-governance schemes: Soil Health Card, Crime and Criminal Tracking Network & Systems (CCTNS), Project Panchdeep, U-Dise, Electronic Health Records, NHRM Smart Card, MyGov, eDistricts, Mobile Seva, Digi Locker, eSign framework for Aadhaar, Passport Seva, PayGov, National Land Records Modernization Programme (NLRMP), and Aadhaar.

The project analyses fifteen schemes that have been rolled out by the government, starting from 2010. The egovernment initiatives by the Central and State Governments have been steadily increasing over the past five to six years and there has been a large emphasis on the development of information technology. Various new information technology schemes have been introduced across the numerous Ministries of the government. The Department of Electronics and Information Technology (DeITY) has been primarily responsible for the development of eGov schemes and has provided technical assistance to other departments for the development of eGov schemes.

The schemes identified for the purpose of this paper have been introduced by the following government agencies:

S. No.	Scheme	Government Agency Involved
1	**SOIL HEALTH CARD** A scheme designed to provide complete soil information to farmers.	Department of Agriculture Corporation (DACNET)
2	**CRIME AND CRIMINAL NETWORK TRACKING & SYSTEMS (CCTNS)** A scheme that seeks to facilitate the functioning of the criminal system through online records, and has proposed data analysis for the purpose of trend setting, crime analysis, disaster and traffic management, etc	National Crime Records Bureau (NCRB)
3	**U-Dise** Serves as the official data repository for educational information.	Ministry of Human Resource Development (MHRD)
4	**PROJECT PANCHDEEP** The use of Unified Information System for implementation of health insurance facilities under ESIC (Employee State Insurance Corporation).	Ministry of Labour & Employment
5	**ELECTRONIC HEALTH RECORDS** A scheme to digitally record all health data of a citizen from birth to death.	Ministry of Health and Family Welfare (MoHFW)

S. No.	Scheme	Government Agency Involved
6	**NHRM SMART CARD** Under the Rashtriya Swasthya Bima Yojana (RSBY) Scheme, every beneficiary family is issued a biometric enabled smart card for providing health insurance to persons covered under the scheme.	Ministry of Health and Family Welfare (MoHFW)
7	**MYGOV** An online platform for government and citizen interaction.	The Department of Electronics and Information Technology (DeITY)
8	**EDISTRICTS** Common Service Centres are being established under the scheme to provide multiple services to the citizens at a district level.	DeITY
9	**MOBILE SEVA** A centralized mobile app, used to host various mobile applications.	DeITY
10	**DIGILOCKER** A scheme that provides a secure dedicated personal electronic space for storing the documents.	DeITY
11	**eSIGN FRAMEWORK FOR AADHAAR** eSign is an online electronic signature service to facilitate an Aadhaar holder to digitally sign a document.	Ministry of Electronic and Information Technology
12	**PAYGOV** A centralized platform for all citizen to government payments.	DeITY and NSDL Database Management Limited (NDML)
13	**PASSPORT SEVA** An online scheme for passport application and documentation.	Ministry of External Affairs
14	**NATIONAL LAND RECORDS MODERNIZATION PROGRAM (NLRMP)** The scheme seeks to modernize land records system through digitization and computerization of land records.	DeITY and NDML
15	**AADHAAR** A scheme for unique identification of citizens for the purpose of targeted delivery of welfare benefits.	Unique Identification Authority of India (UIDAI)

India is at its nascent stages in developing privacy laws and the jurisprudence around the same is still evolving. Section 43A of the Information Technology Act, 2000 and the associated Information Technology Rules (Reasonable security practices and procedures and sensitive personal data or information) 2011 mandates body corporates to protect privacy and to adopt reasonable security practices. The Act also provides for punishment for breach of privacy and confidentiality [4], compensation for failure to protect data [5], punishment for identity theft [6], punishment for violation for privacy [7], etc. Through the Act, the Government has also been granted the power to issue directions for interception or monitoring or decryption of any information through any computer resource [8], power to issue directions for blocking for public access of any information through any computer resource [9], power to authorize monitoring and collection of traffic data or information through any computer resource for cyber security [10], lay down modes or methods for encryption [11], etc.

The Information Technology Rules (Reasonable security practices and procedures and sensitive personal data or information) 2011 have been made applicable only to body corporates [12] but the same standards have not been made applicable to governmental bodies. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 lay down a definition of SPDI (sensitive personal data or information) [13] and mandate body corporates to instate a policy for privacy and disclosure of information. [14] The rules also lay down provisions for the collection of information [15], disclosure of information [16]. The problems identified in this paper arise not only because of inadequate standards, but also due to the absence of standards *in toto*. Despite the Information Technology (Intermediaries guidelines) Rules, 2011, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Information Technology Act, 2000 (Electronic Service Delivery Rules 2011) and the Information Technology Act, 2000, there is no binding obligation upon the Central or State government to comply with privacy standards. Though it is possible that the government is the largest collector of such personal information, it continues to lack the same privacy standards that have been imposed upon private parties.

Methodology

For the purpose of this paper, publicly available information has been collected from the different schemes in order to chart the flow of data upon collection from citizens via the government and private agencies. The documents that the government has made available in the public domain for the citizens have been used to assess the standard of transparency and openness of the government and their level of accountability towards its citizens. This paper seeks to identify the potential privacy gaps in the Digital India schemes based on general privacy and data protection standards. For each project, we seek to gather the following information in order to gauge the standards of data protection and privacy and clearly understand the data flow in the scheme:

- the date of commencement of the scheme,
- the governmental agency involved in the scheme,
- whether a privacy policy under the scheme has been made available to the public,
- whether consent forms have been taken from the users,
- what data is collected under the scheme,
- whether the data collected under the scheme includes sensitive personal data or information (SPDI),
- the method in which information collection is done under the scheme,
- the use of information under the scheme,
- the policies on information disclosure made available under the scheme,
- information on retention of information under the scheme,
- information storage under the scheme,
- security measures devised under the scheme and,
- the involvement of private companies in the egov schemes.

Based on the above data collected for each scheme, the paper analyses the nature and extent of privacy gaps through these schemes.

Privacy Policy

It is observed that in eleven out of fifteen schemes [17], no specific privacy policy has been laid down that has been made available to the public. While general regulations may be followed in each scheme, no specific privacy guidelines are followed universally through these schemes, and they fail to take into account the recognizable privacy harms that the users are subjected to.

For example, in the CCTNS project, in some states the NCRB has reported that steps are being taken for data privacy, confidentiality and access control. [18] However, no specific principles have been laid down by the agencies. The NHRM Smart card rolled out under the RSBY encrypts and duplicates data to protect the large amount of medical information collected, but no specific privacy

policy has been made available. In these schemes, selective privacy principles have been laid down, but it is clear that no policy has been laid down to prevent the recognizable harms from a possible privacy breach.

Out of the four schemes that have laid down comprehensive privacy policies, measures taken by the UIDAI are backed by a statute [19], whereas in the case of electronic health records [20] and the eSign framework for Aadhaar [21] and CCTNS rules have been framed by the executive. For the regulation of Electronic Health Records, a detailed policy has been laid down under the National Health Policy Draft, 2015. This includes the adoption of National Electronic Health Record Standards (announced by the Ministry in 2013) and Metadata and Data Standards. [22] The eSign framework for Aadhaar is governed by the Electronic Authentication Technique and Procedure Rules, 2015. [23] Privacy measures taken under this scheme include the use of one way hash of the documents, use of public key verification, etc. [24] The UIDAI has to follow the regulations laid down under Chapter IV of the Aadhaar Act, 2016, and it encapsulates specific principles to be followed. [25] In Project Panchdeep, an access control policy has been laid down for granting access, access transfer, and access termination. [26] The ISO 27001 Information Security Management System is to be followed. [27] However, there is no specific policy laid down to account for subsequent protection of data after access to data has been granted.

Consent Forms Taken

Informed consent for the use of information is an important principle of privacy. However, no such data is available to indicate that explicit consent is being taken from citizens. None of the schemes examined under this paper take explicit consent forms from its users. Instead, it appears that consent is assumed when an individual signs up or engages in a service. In cases of schemes like DigiLocker, the flow of information and its use is contingent upon the request of the user. Access to the data collected in these schemes is given upon the intimation of the user. Under the Aadhaar scheme, the enrolment form contains a consent column for the user to expressly consent to use of their biometric information or not. [28] However, the user is not made aware of the potential use of information, as the Aadhaar card is increasingly being made mandatory for availing welfare schemes. [29]

In other schemes, however, no specific consent forms are filled out while enrolling in the scheme. The flow of information is still contingent upon the request of the user. However, in any given situation, if the authority collecting data decides to use the information for any other purpose or link it to another database, no provision has mandating the seeking of consent from the user.

Data Collected

The data collected under the various schemes include a variety of personal data including personally identifiable information that they are forced to disseminate in order to avail the benefits of the governmental welfare schemes. In all schemes, personal information of the users are collected. The nature of information collected varies from scheme to scheme depending on its requirements. This data is mostly collected at the district or state level from the individuals, and is collated by the centre.

For example, the data collected under CCTNS includes the information collected in prisons, forensic science labs, courts, prosecution records and police stations. [30] The data collected by the various state data centres will be subsequently linked to the National Data Centres. Under the NHRM Smart Card, the data collected includes personal details of the families that are listed as beneficiaries, photographs, demographic information, settlement details, insurance details, hospital details. etc. [31]

Sensitive Personal Data or Information (SPDI)

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 is the only legislation that has defined SPDI (sensitive personal data or information). Under Section 3, the legislature has listed the data that can classify as SPDI. Eleven out of fifteen schemes collect SPDI. [32] Biometric information, mostly fingerprints, are collected under CCTNS, Aadhaar, Project Panchdeep, NHRM Smart card, Digilocker, NLRMP, eSign framework for Aadhaar, Passport Seva. Medical records are collected under the Electronic Health Records scheme and CCTNS (physiological and psychological data on convicts). Paygov collects the bank account details of its users.

Information Collection

The information is either collected afresh from the source or from pre-existing historical records.

a. Pre-existing records (existing legacy data in physical or electronic forms) – CCTNS,, Electronic health records, NHRM Smart card (pre-existing census data), Digilocker, NLRMP

b. Freshly collected – soil information freshly collected (Soil Health Card), Project Panchdeep, UDISE, Electronic Health Records, NHRM Smart card (The Transaction Management Software (TMS system) being used at the hospital to collect data), MyGov, eDistricts, Mobile Seva, PayGov, Digilocker (information is voluntarily updated by user), eSign (information is voluntarily updated by user), Passport Seva (Through online application made voluntarily by the applicants), Paygov (Information is collected through an online platform set up by the NSDL Database Management Limited), NLRMP, Aadhaar

In order to store this information electronically, data digitization and datafication processes are being carried out in many of these schemes including, CCTNS, Electronic Health Records, NLRMP, UDISE, etc. The information that is freshly collected is also often collected in electronic forms in order to facilitate the digitization process. This facilitates faster data analysis using big data tools and other IT software.

Information Disclosure

Due to the lack of privacy policies in these schemes, these projects do not have policies on the disclosure of information. As a general policy, the information would only be disclosed upon the request of the user depending on their requirements. For example, under Digilocker, information uploaded by the user will be disclosed upon the request and consent of the user for the purpose specified by the user.[33] In this manner, the use of information and the disclosure of the personal information should be contingent upon the request of the customer. However, there is no policy to regulate information disclosure by the government and private agencies involved on their own accord. Further, Section 29 of the Aadhaar Act prohibits disclosure of identity information without consent of the user. Section 29(1)(b) states that "No identity information available with a requesting entity shall be - disclosed further, except with the prior consent of the individual to whom such information relates."[34] The Section restricts sharing of information, particularly biometric information for any other purpose that specified under the Act or through Regulations.[35] Policy on information disclosure is not available in any other schemes.

Information Retention

In six out of fifteen schemes, the electronic data is retained and stored. Due to the digitisation of records, retention of information and data analysis has become easier. Furthermore, this increases the availability of historical data records, thereby assisting the policy makers in better decision making. In the remaining schemes, there is a lack of clarity on whether the information is retained. However, no specific policy on protection of such information that is retained has been made available, which indicates that the information is susceptible to data threats.

The information in eDistricts[36] and NLRMP[37] are retained in a centralised data repository. Subsequent to the eDistrict Scheme, the Registrar General of India & Census Commissioner (RGI), Ministry of Home Affairs, Government of India, is adopting a centralized Birth and Death Registration Software across the country to overcome some major bottlenecks in the collection of Birth and Death Data.[38] In NLRMP, a UNICODE data storage standard is used.[39] The PayGov scheme has collaborated with the NSDL Database Management Ltd (NDML) for infrastructural assistance through which details of transactions are stored.[40] Cloud services are being used under DigiLocker to permanently retain the information and to increase access to such information at all times.[41] The data that is retained also includes the SPDI. For example, the eSign Framework for Aadhaar retains the digital signature of the user and uses the DigiLocker services to store the same.[42] Even in Aadhaar, the UIDAI permanently retains the biometric information of the user in the CIDR.[43]

Information Stored

Provisions have been made to store data in eleven out of the fifteen schemes. Under the Aadhaar, data stored in the Centralised Identities data repository (CIDR) and the authority is required to secure and protect against access, use or disclosure that is not permitted under the Act or regulations made thereunder.[44] In eight of these schemes, information is retained and stored by the Government. Under Digilocker, there is cloud storage of information and Aadhaar seeding to the CIDR for verification purposes.[45] The information collected from various states in the eDistricts scheme is stored in central repository.[46] In the Mobile Seva schemes, information is stored on the cloud. eSign framework retains the electronic signatures.[47] Under Passport Seva[48], NRLMP[49], & Paygov[50], the information is stored in Centralised databases. With the advancement in technology, cloud storage of information has become more popular in order to increase the accessibility of the stored information and also for better data retention.

In some schemes, databases are being linked, providing access to information across governmental departments. For example, under CCTNS, the database is being linked with UIDAI, NPR and the Transport database.[51]

Security Measures

In seven schemes, there is a complete vacuum in security measures to protect the data collected from the citizens. Out of the remaining schemes, security measures are undertaken to some limited extent in three schemes.

Under the CCTNS scheme, a security review is conducted to assess the data access privileges, retention periods and archival mechanisms in some states like Karnataka.[52] In Chhattisgarh, the CCTNS application security initiative includes DMZ Policy, encryption, authentication, authorization and digital signature.[53] NHRM Smart Card has set up a network firewall - Cisco ASA 5580 Series and a server farm protection firewall used.[54] A security monitoring and co-relation appliance is also used.[55]

Under U-DISE, the software provides facilities for school code generation, which is unique and consistent with various administrative levels.[56] This unique school code for every student ensures the unique identity of every student enrolled, and ensures accuracy in the enrolment of the scheme.[57] Under the Electronic health records, Interoperability Standards are used as a security measure, along with components of both public and private key encryption.[58] Under eDistricts, the security initiatives may include PKI infrastructure, DMZ Policy, encryption, authentication, authorization and digital signature.[59] NLRMP has laid down international standards - ISO/IEC 27001 and ISO/IEC 27002 as a security standards.[60] For the UIDAI, Sections 28-33 of the Aadhaar Act, 2016 lay down detailed security measures to be followed[61]

Involvement of Private Companies

In eleven schemes, there is no report of any involvement of private party, whereas in four schemes, private companies have played an integral role in the functioning of the schemes. Digilocker makes use of third party service providers as Certifying Authorities (CA) licensed as per the IT Act under the Controller of Certifying Authorities (CCA).[62] Tata Consultancy Services (TCS) provides assistance for the Passport Seva Kendra.[63]

Under the CCTNS scheme, private System Integrators are appointed in each State, for example Rotla[64], Wipro Infotech[65], etc. The eSign framework for Aadhaar uses third party service providers, like Certifying Authorities (CA) licensed as per the IT Act under the Controller of Certifying Authorities (CCA).[66] Under the Aadhaar project, the involvement of private parties has been criticized over the years. Private parties are allowed to act as 'requesting authorities' under the Act, to utilize the Aadhaar database for verification and identification purposes. In a petition raising privacy concerns under the Aadhaar scheme, the Supreme Court observed that 'biometric data collection by private agencies if not a good idea.'[67]

Information Use

The information that is collected is envisaged to be used only for the purpose that it is collected for. In all instances these welfare schemes collect information for the end benefit of the user, and the data that is collected is used to provide benefits to the users. The data also contributes to the government's repository of data for better policy decisions through data analysis. The use of information is specific to the scheme and also benefits the enforcement agencies in identification of the right beneficiaries for the scheme by building a target group for the same. In some schemes, the information is also used for tracking purposes through data analysis – tracking soil conditions, tracking criminals, tracking diseases through health information, etc.[68]

Data is available to track the use of information under each scheme as stipulated by the concerned department. The use of such information is specific to the scheme. However, there are no policies to restrict the use of the data collected for the purpose of the scheme. In some instances, the use of information expands as the scope of the scheme expands. For example, under Aadhaar the linking and seeding of databases were not earlier envisaged when the project was rolled out. The users were not made completely aware of the potential use of information collected by the UIDAI and neither were subsequent consent forms taken for this purpose. Even under the CCTNS scheme, the data collected could be potentially used for predictive analysis. With the continuous development of technology and the assimilation of large quantums of data, the use of information under each scheme will continue to develop.

Conclusion

The Digital India project aims to enhance the delivery of services to the citizens at the cost of exposing their personal information to cyber security threats. The lack of available information and the inadequacy of security measures in these welfare schemes raises questions on the transparency in the functioning of these schemes and their overall efficiency. The standards applied by the government while dealing with large quantums of personal data and SPDI are abysmal as most schemes lack privacy policies and security measures. The absence of a legislation also results in a vacuum for redressal mechanisms in

cases of privacy breaches. The large quantum of data stores is susceptible to the rising cyber security threats, especially with the lack of stringent policies on information storage, information retention and information disclosure.

The transparency levels of the government are also reflected through the data collected, as it is not possible to trace the data flow in many schemes. Only under Aadhaar is data available on the flow of information as it is backed by a statute. The least degree of transparency in data flow is seen in the MyGov scheme as this scheme does not collect personal information or SPDI. In all schemes, the data most available includes the data collected, information collection and information use. The least amount of data available is on information disclosure policies under these schemes. The most recorded privacy gaps based on the available data can be seen in Aadhaar and CCTNS, while the least in Mobile Seva and eDistricts.

The success of these schemes is backed by the advancement of technology, but fall back based on the vacuum of privacy policies and security measures. As already noted, the citizens lack clarity of information on the manner and method in which their personal information and SPDI is currently being used. In such situations, there can never be any informed consent from the citizens on the use of their personal data. While India is making quick progress in its technological advancement, it is still struggling to balance the rights of its citizens against its push for digitization. Transparency in government activities is pivotal in all democratic processes, and the lack of the same is evident through the data presented in this paper. Further, the requirement of privacy policies and security measures is a *sine non qua* to protect the citizens from potential cybersecurity threats and misuse of power in the hands of the government and private parties.

ENDNOTES

1. Introduction to Digital India, *available at* http://www.governancenow.com/news/regular-story/securing-digital-india.
2. *Id.*
3. GN Bureau, *Securing Digital India*, Governance Now (June 11, 2016) *available at* http://www.governancenow.com/news/regular-story/securing-digital-india.
4. Information Technology Act, 2000, Section 72.
5. Information Technology Act, 2000, Section 43A
6. Information Technology Act, 2000, Section 66C
7. Information Technology Act, 2000, Section 66E
8. Information Technology Act, 2000, Section 69
9. Information Technology Act, 2000, Section 69A
10. Information Technology Act, 2000, Section 69B
11. Information Technology Act, 2000, Section 84A
12. Information Technology Act, 2000, Section 43A
13. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Section 3
14. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Section 4
15. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Section 5
16. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Section 6
17. Note: Privacy policies are available in Aadhaar, CCTNS, eSign Framework for Aadhaar, Electronic Health Records. No information on any privacy policy has been made public in Passport Seva, Project Panchdeep, Mobile Seva, U-DISE, eDistricts, MyGov, Soil Health Card, DigiLocker, NLRMP, NHRM Smart Card and PayGov.
18. Chhattisgarh RFP, Implementation of CCTNS Project in Chhattisgarh, Vol. I, *available at* http://ncrb.nic.in/BureauDivisions/CCTNS/All%20State%20RFP/Chhattisgarh/CG_CCTNS_RFP_Vol-I%20Functional%20&%20Technical%20Specifications.pdf.
19. The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.
20. *Circular on Electronic Health Records Standards for India*, Ministry of Health and Family Welfare (August 2013) *available at* http://www.mohfw.nic.in/showfile.php?lid=1672.
21. *eSign-Online Digital Signature Service*, Ministry of Electronics and Information Technology (Controller at Certifying Authorities) *available at* http://www.cca.gov.in/cca/?q=eSign.html.
22. *Supra* at 17.
23. Note: Section 2 of the Rules, provide for compliance with the Digital Signature (End entity) Rules, 2015 in so far as they relate to the creation, storage, and verification of Digital Signature.

24. *Supra* at 21.

25. *Supra* at 19.

26. Wipro Press Release, *Wipro Completes Implementation of Employees' State Insurance Corporation (ESIC) "Project Panchdeep"* (Feb. 24, 2012) *available at* http://www.wipro.com/newsroom/press-releases/Wipro-completes-implementation-of-Employees-State-Insurance-Corporation-ESIC-Project-Panchdeep/.

27. Request for Proposal, Employee State Insuarance Company, Volume I available at **esic**.nic.in/backend/writereaddata/tenders/RFP_Volume_1.pdf.

28. Aadhaar Enrolment Form, *available at* https://uidai.gov.in/images/uid_download/enrolment_form.pdf.

29. Gopal Kirishna, *UID/Aadhaar Enabled Bio-Metric Attendance System (AEBAS) Violates Supreme Court's Orders*, (Jan. 10, 2017) *available at* http://www.livelaw.in/uidaadhaar-enabled-bio-metric-attendance-system-aebas-violates-supreme-courts-orders/.

30. Office Memorandum, Ministry of Home Affairs, (Dec. 22, 2015) *available at* http://mha.nic.in/sites/upload_files/mha/files/CCTNSMHA_11012016.pdf

31. About RSBY, Rashtriya Swasthya Bima Yojana, *available at* http://www.rsby.gov.in/about_rsby.aspx.

32. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Section 3.

33. *How Digital Locker Works - A Brief Introduction*, DigiLocker, *available at* http://digilockers.in/how-digilocker-works/.

34. The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 29(1)(b).

35. The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 29.

36. eDisrtict Mission Mode Project under The National eGovernance Plan, *Pilot Information Guidelines*, Department of Information and Technology (Jan. 2009) *available at* http://nisg.org/files/documents/A05040001.pdf.

37. The National Land Records Modernization Programme (NLRMP), *Guidelines, Technical Manuals and MIS*, Ministry of Rural Development (2008-09) *available at* http://dolr.nic.in/Guidelines%20%20NLRMP%2017.4.2009.pdf.

38. Office Memorandum - *Advisory on Implementation of Birth and Death Services under the eDistrict Project, Ministry of Communication and Technology*, (Dec. 18, 2014) *available at* http://meity.gov.in/sites/upload_files/dit/files/Advisory_Birth_Death_Certificates_Dec2014.pdf.

39. *Supra* at 29.

40. *PayGov India National Payment Service platform*, Ministry of Electronics and Information Technology, *available at* http://meity.gov.in/content/paygov-india-national-payment-service-platform.

41. Ankur Aggarwal, *Can Digital Locker Catalyze Digital India*, Maximum Governance (Sept. 4, 2016) *available at* http://maximumgovernance.com/perspectives/digilocker-is-a-potential-digital-india-catalyst/.

42. eSign FAQ, *available at* http://cca.gov.in/cca/sites/default/files/files/ESIGNFAQFeb26022015.pdf.

43. The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 28(3).

44. *Id*.

45. *Supra* at 34.

46. *Supra* at 29.

47. *Mobile Applications and M-Gov Application Store*, Ministry of Electronice and Information Technology, *available at* https://mgov.gov.in/msdp_appstore.jsp.

48. Mohd. Ujaley, *The Digital Makeover of the Indian Passport*, The Financial Express, (March 28, 2016) *available at* http://www.financialexpress.com/industry/technology/the-digital-makeover-of-indian-passport/229995/.

49. *Supra* at 30.

50. *Supra* at 33.

51. Cabinet Committee on Economic Affairs (CCEA), *Extension of Crime and Criminal Tracking Network and Systems Project,* (Nov. 18th 2015) *available at* http://pib.nic.in/newsite/PrintRelease.aspx?relid=131585.

52. CCTNS RFP for State System Integrator Karnataka, eGovernance MMP of MHA, GoI, *available at* http://www.slideshare.net/sahaysanjay/karnataka-state-police-rfp-volume-1.

53. *Supra* at 15.

54. *RSBY Operational Guidelines*, Ministry of Labour & Employment, *available at* http://rsby.gov.in/Docs/Guidelines%20for%20Revamp%20of%20RSBY%20-Operational%20Manual%20for%20Phase%20I%20(Released%20on%2016th%20July%202014).pdf.

55. *Id*.

56. National University of Educational Planning and Administration, Sample

Checking OF U-DISE 2015-16, *available at* http://dise.in/Downloads/Sample%20Checking/Sample_Checking_DCF_2015-16.pdf.

57. *Id.*

58. Department Of Health And Family Welfare – *Circular on Electronic Health Records Standards in India*, Approved by the Ministry of Health and Family Welfare, *available at* http://www.mohfw.nic.in/showfile.php?lid=1672.

59. *Supra* at 29.

60. *Supra* at 30.

61. *Supra* at 16.

62. *Digital Signature Certificate Enrollment User Manual*, PFMS, Controller General of Accounts Ministry of Finance (May 4, 2016) *available at* http://dolr.nic.in/dolr/downloads/pdfs/DSC_Enrollment_User_Manual_v2.1.pdf.

63. *Supra* at 41.

64. *Emergency Response Management: Changing the Paradigm of Public Safety Management*, Rotla, *available at* http://www.rolta.com/solutions/safety-security-solutions/emergency-response-management/.

65. Wipro Press Release, *Home Ministry Selects Wipro to Develop Core Software for Crime and Criminal Tracking Network System (CCTNS)*, (Aug.2, 2010) *available at* http://www.wipro.com/newsroom/press-releases/Home-Ministry-selects-Wipro-to-develop-core-software-for-Crime-and-Criminal-Tracking-Network-System-CCTNS/.

66. *eSign – Online Digital Signature Service*, Ministry of Electronics and Information Technology, *available at* http://www.cca.gov.in/cca/?q=eSign.html.

67. Live Law Networks, *Aadhaar; Data collection by private agencies not a good idea: SC*, (Jan. 5th, 2017) *available at* http://www.livelaw.in/aadhaar-data-collection-private-agencies-not-good-idea-sc/.

68. Note: Data compiled from RFPs of different states.

Digital India Schemes

Passport Seva

Date of Commencement **2010** | Government Agency **Ministry of External Affairs**

No privacy policy has been made available under this scheme. There is no information on whether the scheme has laid down any specific security measures and whether they have policies on data disclosure and data retention. In the absence of such policies, the storage of information by the Passport Seva Kendra and the linking of the database with Aadhaar poses privacy threats as there is neither a privacy policy nor security measures in place. Further, as there is collection of SPDI and private companies are involved, the lack of any comprehensive policy indicates privacy gaps. As there are no policies on information retention and information disclosure, the data may be susceptible to misuse.

PRIVACY POLICY

DATA COLLECTED

In addition to the existing information collected in passport applications, the e-application also collects the Aadhaar number, which is synced to the UID database.

SPDI

Biometric information

INFORMATION COLLECTION

Information is collected online, directly from the Passport applicants.

INFORMATION USE

- Online application for passports
- Online application for Police Verification

INFORMATION DISCLOSURE

INFORMATION RETENTION

INFORMATION STORED

- All information that is collected is stored in the Passport Seva Kendra
- The biometric information collected is stored in the UID database

(A proposal has been made to store the information in a chip.)

SECURITY MEASURES

INVOLVEMENT OF PRIVATE COMPANIES

The Government has entered into a Public Private Partnership (PPP) with TCS for this project.

Aadhaar

Date of Commencement **2010** | Government Agency **Unique Identification Authority of India**

Due to the enactment of the Aadhaar Act, the data flow can be traced through the statutory provisions laid down by the legislature. The collection of SPDI, and its retention and storage poses privacy threats, especially with the involvement of private companies. Further, the linking and seeding of large databases to Aadhaar potentially may face security threats, due to rising rate of cybercrimes and the nature and sheer quantum of data collected.

PRIVACY POLICY

The privacy policy is governed by Chapter IV of the Aadhaar Act, 2016.

DATA COLLECTED

Demographic information, personal information and biometric information

SPDI

Fingerprints, Retina scans

INFORMATION COLLECTION

First hand information is collected at source, through the Aadhaar camps.

INFORMATION USE

- Aadhaar card is used as a Proof of Identity
- Used for verification purposes in order to avail welfare schemes of the Government

INFORMATION DISCLOSURE

Governed by the Aadhaar Act (S29 - identity information not to be disclosed without consent)

INFORMATION RETENTION

Information is retained in the UID Database

INFORMATION STORED

Information is stored in the centralized database called 'Central Identities Data Repository' (CIDR)

SECURITY MEASURES

Section 28-33 of the Aadhaar Act lay down the security measures that are required to be followed.

INVOLVEMENT OF PRIVATE COMPANIES

Private parties are using the CIDR for identity verification purposes.

Crime and Criminal Network Tracking & Systems (CCTNS)

Date of Commencement **2012** | Government Agency **National Crime Record Bureau**

The scheme lacks a specific privacy policy. The System Integrators in each state are required to have policies on data privacy, confidentiality and access control while formulating the scheme. SPDI is collected from the citizens for the purpose of this scheme, and despite that the security measures laid down are inadequate. The storage of data and the involvement of private companies in this project, in the absence of any comprehensive privacy policy poses various privacy threats due to the potential misuse of SPDI, as there are no uniform standards laid down across all states. Further, more stringent security measures are required when there is information storage of such large databases in the National Data Centres, in order to prevent cyber threats. As there are no policies on information retention and information disclosure, the data may be susceptible to misuse.

PRIVACY POLICY

No specific policy made available. However, steps are being taken for data privacy, confidentiality and access control.

DATA COLLECTED

Data collected includes data on crimes, criminals, evidence and scientific reports, case details from police stations and courts, prison details, statistical data, biometric information, etc.

SPDI

- May include biometric information, medical reports related to the crime
- May also include physical, physiological and mental health condition of convicts

INFORMATION COLLECTION

- Existing legacy electronic data
- Data taken from existing registers, reports, case files
- Images and pictures within the case files
- FIR, Charge Sheet, Seizure Memo, Conviction Memo, Arrest Memo
- Crime (case/incident) data, criminals' data, the data from the police stations records rooms (from police registers).
- Citizen complaint information

INFORMATION USE

Tracking, investigation and analysis of crimes.

INFORMATION DISCLOSURE

INFORMATION RETENTION

Information is being digitized in order to be retained in electronic databases.

INFORMATION STORED

State Data Centres are being created, which will be ultimately linked to a National Data Centre for this purpose.

SECURITY MEASURES

- A security review is conducted to assess the data access privileges, retention periods and archival mechanisms.
- CCTNS application security initiatives should include, DMZ Policy, encryption, authentication, authorization and digital signature.

INVOLVEMENT OF PRIVATE COMPANIES

Private System Integrators (SI) are appointed in each state. Eg. Wipro Infotech, Rotla, etc.

Mobile Seva

Date of Commencement **2012** | Government Agency **DeITY**

The collection of SPDI in the absence of a privacy policy and security measures, poses potential threats and indicates a privacy gap. Lack of policies on information disclosure and information stored also raise questions on potential privacy breaches under the scheme.

PRIVACY POLICY

DATA COLLECTED

Data is collected depending on the service that is rendered.

SPDI

Possible collected of medical records under mSwasthya.

INFORMATION COLLECTION

Information is collected online, directly from the user.

INFORMATION USE

Delivery of public services to citizens and businesses over mobile devices using SMS, USSD, IVRS, CBS, LBS, and mobile applications.

INFORMATION DISCLOSURE

INFORMATION RETENTION

INFORMATION STORED

SECURITY MEASURES

INVOLVEMENT OF PRIVATE COMPANIES

Project Panchdeep

Date of Commencement **2012** | Government Agency **Ministry of Labour & Employment (under ESIC)**

Privacy gaps arise where there is sufficient collection of SPDI, but insufficient security measures and a comprehensive privacy policy to govern the use of such SPDI. As there are no policies on information retention and information disclosure under the scheme, the data may be susceptible to misuse.

PRIVACY POLICY

- ISO 27001 Information Security Management System to be followed.
- Access control policy for access, granting access, access transfer, and access termination.

DATA COLLECTED

Details of the insured person and family, Hospitals, Labs, Insurance details

SPDI

Biomertic data

INFORMATION COLLECTION

Information collected from source and existing historical data

INFORMATION USE

- Data collected on the card - verification and authentication purposes.
- The electronic medical health records are used by hospitals to check the previous medical history of the IP that is to facilitate better medical treatment
- Accessed by the insurance solutions to process the insurance claims.

INFORMATION DISCLOSURE

INFORMATION RETENTION

INFORMATION STORED

SECURITY MEASURES

- Network firewall - Cisco ASA 5580 Series
- Server Farm protection Firewall used
- Security Monitoring and co-relation appliance used

INVOLVEMENT OF PRIVATE COMPANIES

U-Dise

Date of Commencement **2012** | Government Agency **MHRD**

The storage of information with the lack of a comprehensive privacy policy and inadequate security measures pose potential privacy threats. As there are no policies on information retention and information disclosure, the data may be susceptible to misuse.

PRIVACY POLICY

DATA COLLECTED

Details of schools, students, teachers, performance levels, condition of the schools, quality of the schools, etc.

SPDI

INFORMATION COLLECTION

Information collected from source

INFORMATION USE

- Data analysis
- Data results used to influence major policy decisions

INFORMATION DISCLOSURE

INFORMATION RETENTION

The information is collected in electronic form and retained.

INFORMATION STORED

Information is stored in a centralised data repository

SECURITY MEASURES

- The software provides facilities for school code generation which is unique and consistent with various administrative levels
- Random Data Sampling is being done by various states since 2005-06 to ensure that the data is reliable and accurate

INVOLVEMENT OF PRIVATE COMPANIES

---

eDistricts

Date of Commencement **2014** | Government Agency **DeITY**

The storage of information with the lack of a comprehensive privacy policy and inadequate security measures pose potential privacy threats. As there are no policies on information retention and information disclosure, the data may be susceptible to misuse.

PRIVACY POLICY

DATA COLLECTED

- Birth and Death data
- Certificates including Domicile, Nativity, Caste, Marriage, Income, Employment, etc.
- Pensions – Social welfare Pensions (Old age, Widow, Handicap, Destitute)
- Revenue Court – including Case listing, Case adjournment, Stay orders, Final orders, Status of execution of orders: Information, Tracking, and filing of misc. applications.
- Public Distribution System, Ration Card related services -including Registration, Change of address, Addition of members, Issue of duplicates etc
- Government dues and recovery as part of Land Revenue – including Issue of notices, Record payments, Track default processes, Updation of treasury receipts etc
- RTI services including redressal of Grievances

SPDI

INFORMATION COLLECTION

Information collected from source and from historical data.

INFORMATION USE

To facilitate Government to citizen services, e-delivery of services, etc.

INFORMATION DISCLOSURE

INFORMATION RETENTION

Information is collected in electronic form and retained.

INFORMATION STORED

Information is permanently stored in the centralized data repository.

SECURITY MEASURES

The security initiatives may include PKI infrastructure, DMZ Policy, encryption, authentication, authorization and digital signature.

INVOLVEMENT OF PRIVATE COMPANIES

MyGov

Date of Commencement **2014** | Government Agency **Dept. of Electronics & Information Technology**

The scheme lacks a privacy policy and information on security measures to be taken for the information collected. The complete absence of such information, along with any policies on information storage, information disclosure, and information retention indicate privacy gaps in the scheme. There is very less transparency on the data flow under this scheme.

PRIVACY POLICY

DATA COLLECTED

Feedback, inputs, advice and ideas from citizens

Information relating to 37 Ministries, 195 tasks, 1, 3100 submissions, 73 blogs, 276 discussions and 20 talks

SPDI

INFORMATION COLLECTION

Information collected through discussion forums, crowd sourcing, opinion polls

INFORMATION USE

- Sharing of consultation papers in the public domain
- Interface with social media platforms
- Consultation in structured framework through pre-defined questionnaire
- Publication of summary of discussion by the user Department
- Free flow consultation through enabling submission of responses to designated email addresses specified in the consultation paper and through discussion threads moderated by the user Department
- Dash Board Analysis

INFORMATION DISCLOSURE

INFORMATION RETENTION

INFORMATION STORED

SECURITY MEASURES

INVOLVEMENT OF PRIVATE COMPANIES

Soil Health Card

Date of Commencement **2014** | Government Agency **DACNET**

The scheme lacks a privacy policy and information on security measures to be taken for the information collected. The complete absence of such information, along with any policies on information storage, information disclosure, and information retention indicate privacy gaps in the scheme. The lack of information made available in the public indicate poor transparency levels under the scheme.

PRIVACY POLICY

DATA COLLECTED

Farmer Details, Soil Details, Weather Conditions, Nutrients, Ground Water Levels, Forest Covers, Market and Transport Network

SPDI

INFORMATION COLLECTION

Information collection from source: directly from the farmers, and agricultural plots. The soil testing is done at soil testing labs.

INFORMATION USE

- Proper diagnosis of soils
- Scientific land use planning
- Soil amendments for judicious use of chemical fertilizer
- Soil, land, water, crop and nutrient management
- Generation of soil health cards for dissemination of soil information to farming community
- Development of Soil Information System
- Optimal utilization of soil resources

INFORMATION DISCLOSURE

INFORMATION RETENTION

INFORMATION STORED

The following information is stored:

- Soil health Conditions
- Package of Practices suitable to Soil Type
- Balanced use of Fertiliser (In-Organic/ Organic)
- Automation of Soil Testing Labs for quick dissemination of results
- Soil Survey
- Organic farming
- Details of Soil testing laboratories
- Expert Advisory
- Grievances redressal

SECURITY MEASURES

INVOLVEMENT OF PRIVATE COMPANIES

Digi Locker

Date of Commencement **2015** | Government Agency **DeITY**

The collection of SPDI in the absence of a privacy policy poses a privacy threat to the biometric information of the user. Further, the storage and retention of information are also exposed to privacy threats, due to the inadequacy of the security measures present under the scheme.

PRIVACY POLICY

DATA COLLECTED

Aadhaar No., OTP, Fingerprints, Mobile numbers

SPDI

Fingerprints

INFORMATION COLLECTION

Information is voluntarily uploaded by the user or obtained from the appropriate government department on the request of the user

INFORMATION USE

- Used as cloud storage of physical documents
- Used for online verification
- Used by various government departments to issue or verify documents related to citizens digitally
- Used to submit a digitally signed copy to a government agency
- Assist in Aadhaar seeding by the government
- Connecting of databases

INFORMATION DISCLOSURE

Information disclosed to the concerned authority upon request of the user for verification of documents.

INFORMATION RETENTION

Information stored through cloud services

INFORMATION STORED

Personal documents like University certificates, Permanent account number (PAN) cards, voter id cards, etc. (depending on what the user seeks to upload online)

SECURITY MEASURES

Use of unique Aadhaar no. to enhance security

INVOLVEMENT OF PRIVATE COMPANIES

---

eSign Framework for Aadhaar

Date of Commencement **2015** | Government Agency **Ministry of Electronics & IT**

Although there is a privacy policy in place, and security measures have been laid down the collection of SPDI creates a security concern when private third parties are involved in the scheme. Despite the Information Technology (Certifying Authorities) Rules, 2000 the retention and storage of electronic signatures can be susceptible to cyber security threats.

PRIVACY POLICY

- Governed by the Electronic Authentication Technique and Procedure Rules, 2015.
- Privacy measures used through use of one way hash of the documents, Public Key verification, etc.

DATA COLLECTED

Name, Address, Email address, Aadhaar e-KYC, Mobile

SPDI

Biometrics or OTP

INFORMATION COLLECTION

Information collected at source, from voluntary applicants.

INFORMATION USE

- Use of eSign by Government agencies, Banks and Financial Institutions, Educational Institutions etc
- Online application for certificates and government documents
- Secure signing of electronic documents

INFORMATION DISCLOSURE

INFORMATION RETENTION

Retention of electronic signature

INFORMATION STORED

- Digital Locker can be used for information storage
- Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 is applied
- Not necessary to store the e-signed record in the e-signature service

SECURITY MEASURES

Issuance of Information Technology (Certifying Authorities) Rules, 2000

INVOLVEMENT OF PRIVATE COMPANIES

Use of third party service provider, like Certifying Authorities (CA) licensed as per the IT Act under the Controller of Certifying Authorities (CCA).

Electronic Health Records

Date of Commencement **2015** | Government Agency **MOHFW**

The collection and storage of medical health records (which constitute SPDI) are exposed to privacy threats, as the security measures laid down are inadequate.

PRIVACY POLICY

Privacy regulations have been laid down. (Exhaustive list available)

DATA COLLECTED

- Personal health information on the patient
- Medication details
- Patient personal details

SPDI

Medical records of the patient

INFORMATION COLLECTION

Information collected at source and from historical medical records

INFORMATION USE

- Providing accurate, up-to-date, and complete information about patients at the point of care;
- Access patient records quickly for more coordinated, efficient care;
- Share electronic information securely with patients and other clinicians
- Diagnose patients more effectively,
- Reduce medical errors and provide safer care;
- Prescribe more reliably and safer;
- Promote legible, complete documentation and accurate,
- Streamlined coding and billing;
- Reduced duplication of testing, and improved health
- The provision of services include – SMS-based services, live and asynchronous telemedicine and interactive voice response service (IVRS)

INFORMATION DISCLOSURE

INFORMATION RETENTION

INFORMATION STORED

SECURITY MEASURES

- Public and private key encryption
- Interoperability standards

INVOLVEMENT OF PRIVATE COMPANIES

National Land Records Modernization Programme

Government Agency **DEITY and NDML**

The scheme lacks a specific privacy policy, although security measures based on international standards have been laid down. The information that is collected is retained and stored in a database. However, there are no specific privacy policies relating to the same, which amounts to a privacy gap. Further, the lack of a policy on information disclosure also amounts to a privacy gap. The collection of SPDI without a privacy policy also raises concerns.

PRIVACY POLICY

DATA COLLECTED

Land record details, Survey details, Registration details

SPDI

During registration of property, fingerprints of the parties and witnesses are captured.

INFORMATION COLLECTION

Digitization of existing data or by conducting fresh surveys

INFORMATION USE

Management of land records

INFORMATION DISCLOSURE

INFORMATION RETENTION

Information collected in electronic form is retained.

INFORMATION STORED

Information is stored in a centralized database.

SECURITY MEASURES

International security standards applied - ISO/IEC 27001 and ISO/IEC 27002.

INVOLVEMENT OF PRIVATE COMPANIES

NHRM Smart Card

Government Agency **MoHFW**

The NHRM Smart card collects SPDI and stores the same on the smart card that is provided to the beneficiary. Despite the various potential threats to the information of the beneficiary, the scheme lacks a privacy policy and security measures. Further no policies on information disclosure and information retention have been made available.

PRIVACY POLICY

DATA COLLECTED

Family details, Hospital details, Claim settlement details

SPDI

Biometric information

INFORMATION COLLECTION

- Beneficiary data taken from the latest Census
- The Transaction Management Software (TMS system) being used at the hospital to collect data

INFORMATION USE

NHRM card used to facilitate insurance facilities to the beneficiaries

INFORMATION DISCLOSURE

INFORMATION RETENTION

INFORMATION STORED

Information stored on the NHRM Smart card.

SECURITY MEASURES

INVOLVEMENT OF PRIVATE COMPANIES

PayGov

Government Agency **DEITY and NDML**

The collection of SPDI under the scheme raises privacy and security concerns as the scheme lacks a privacy policy and has limited security measures in place to protect the banking details of the user. While the information is retained and stored in a database, no specific policies have been laid down for information retention and information storage. Further, the scheme lacks a policy on information disclosure which also amounts to a privacy gap.

PRIVACY POLICY

DATA COLLECTED

Credit Cards, Debit Cards, Net Banking details, IMPS (Immediate Payment Services), Cash-card/ Prepaid Card/ Wallets, NEFT/RTGS

SPDI

Credit and Debit card details

INFORMATION COLLECTION

Information is collected through an online platform set up by the NSDL Database Management Limited

INFORMATION USE

Payment and Settlements

INFORMATION DISCLOSURE

INFORMATION RETENTION

Information collected in electronic form is retained.

INFORMATION STORED

Information is stored in the database.

SECURITY MEASURES

Encryption during transmission of data

INVOLVEMENT OF PRIVATE COMPANIES

Tabulation of available data under the schemes and the identifiable privacy gaps

Scheme	Privacy Policy	Data Collected	Information Collection	Information Retention	Information Disclosure	SPDI	Information Stored	Involvement of Private Companies	Information Use	Security Measures
PASSPORT SEVA										
AADHAAR										
CCTNS										
MOBILE SEVA										
PROJECT PANCHDEEP										
U-DISE										
eDISTRICTS										
MYGOV										
SOIL HEALTH CARD										
DIGI LOCKER										
eSIGN FRAMEWORK FOR AADHAAR										
ELECTRONIC HEALTH RECORDS										
NLRMP*										
NHRM SMART CARD										
PAYGOV										

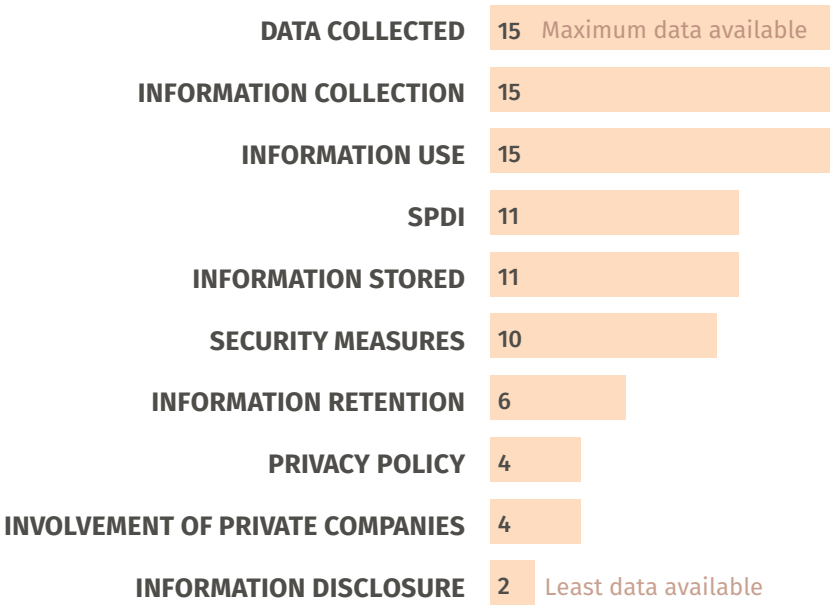
***NLRMP:** NATIONAL LAND RECORDS MODERNIZATION PROGRAMME

No information is available

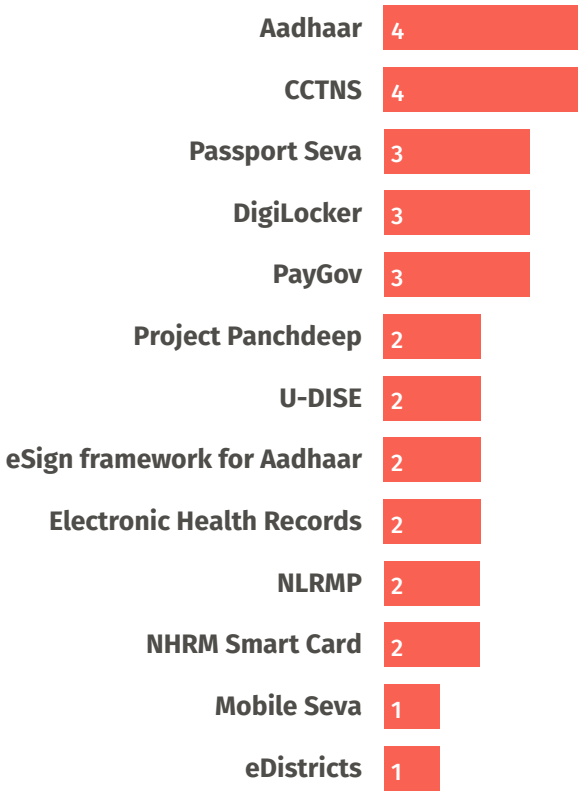
Information is available

Privacy Gap

Ranks in terms of maximum data available



Ranks in terms of most privacy gaps



Ranks in terms of schemes with most transparency based on the data flow that has been made available in the public domain

Aadhaar Most transparency on data flow (as it is governed by a statute)

eSign Framework for Aadhaar

CCTNS, DigiLocker

NLRMP, PayGov

Passport Seva, eDistricts, Electronic Health Records

Project Panchdeep, U-DISE, NHRM Smart Card

Mobile Seva, Soil Health Card

MyGov Least transparency on data flow (Data collected doesn't include a large quantum of personal information)