

By Email/ Post

To,  
Shrimati Kavita Bhatia,  
Scientist F,  
Ministry of Electronics and Information Technology  
Email id: [khatia@gov.in](mailto:khatia@gov.in)  
CC: [pmu.etech@meity.gov.in](mailto:pmu.etech@meity.gov.in)

Dated: March 17, 2022

IFF/2022/019

Dear ma'am,

**Re: Further comments on Policy Document and MeitY Website Change for Draft India Data Accessibility & Use Policy, 2022**

1. We are writing to you to express our concern on the substantial changes made to the Draft India Data Accessibility & Use Policy, 2022 (Draft Data Access Policy) which have not been publicly acknowledged. These changes came as a surprise to us as we noticed version changes on the Draft Data Access Policy on the URL <https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022> as was first uploaded and published on February 21, 2022 and that which was then accessible on March 6, 2022. The version uploaded in or around February 21, 2022 continues to be accessible. These changes can be verified from placing the URL in the WayBackMachine.<sup>1</sup> On further clicking the link to the Draft Data Access Policy from the snapshot dated March 10, 2022 a different version is provided to when a snapshot is accessed dated February 21, 2022 and thereafter. This clearly evidences a verifiable basis to our claim that a public, government document that has been put for public consultation was changed without notice to stakeholders.
2. The objective of the Draft Data Access Policy drafted by the Ministry of Electronics and Information Technology (MeitY) is to utilise data to improve the quality of governance and service delivery as well as to promote innovation. While we commend the objective, we feel it can only be achieved from a rights centric framework. Our principal recommendation, sent to you on March 4, 2022 (IFF/2022/012), is that MeitY reconsider this policy and aim to withdraw it.<sup>2</sup> This is on account of four primary reasons, a) lack of

<sup>1</sup> 'Draft India Data Accessibility & Use Policy 2022' (*WayBack Machine*, 21 February 2022)  
<<https://web.archive.org/web/20220221100523/https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022>>  
accessed on 17 March 2022

<sup>2</sup> 'Comments on Draft India Data Accessibility & Use Policy, 2022' (*Internet Freedom Foundation*, 4 March 2022)  
<<https://drive.google.com/file/d/125LspShPQmZyRDp-PCZuRnTe76Nfd-/j/view?usp=sharing>> accessed 16 March 2022

transparency and faulty consultation process followed; b) privacy concerns with respect to enhanced data sharing; c) primary objectives undergirded by perverse economic objectives; and d) ambiguous definitions and the resultant arbitrariness. A copy of IFF's comments on the Draft India Data Accessibility & Use Policy, 2022 have been annexed herewith and marked as **Annexure 1**.

3. While these concerns remain, we also want to raise serious alarm regarding the multiple changes made to the webpage related to the consultation and the accompanying policy documents. As mentioned on the MeitY website, the Draft Data Access Policy was published on February 21, 2022. This consisted of a 'Background Note' and the policy document. However, recently we noticed various key changes have been made to the policy document and the MeitY webpage where the Draft Data Access Policy was uploaded. A comprehensive list of changes between the two documents has been attached herewith and marked as **Annexure 2**.
4. Here, our principal issue is that these changes have been without any notice or public acknowledgement by MeitY. Such actions leave citizens confused over the purpose and impact of the Draft Data Access Policy. They have practical impacts as preventing stakeholders any extended timeline, varying responses due to varying versions of the Draft Data Access Policy. The present publication also causes misrepresentation as the existing version of the Draft Data Access Policy is distinct from the version first published, however to any casual observer it would be evident that any changes were made. These version changes and the subsequent lack of transparency and accountability is a result of MeitY's failure to abide by the provisions of the Pre-Legislative Consultation Policy, 2014 formulated to incorporate stakeholder perspective and increase transparency.<sup>3</sup> Moreover, such actions inspire a lack of trust in the consultation given that several facial changes were made during the consultation period after receiving criticism from civil society experts.<sup>4,5</sup> Consequently, IFF filed a Right To Information (RTI) application with MeitY to obtain information regarding the time and date when the MeitY website and the policy document was updated, and the specific changes made.<sup>6</sup>

---

<sup>3</sup> Pre-legislative Consultation Policy (PLCP) 2014

<sup>4</sup> TR Raghunandan, 'Will the proposed Data Accessibility Policy free more data, or lock it up tighter behind legalese?' (*MoneyControl*, 28 February 2022)

<<https://www.moneycontrol.com/news/business/will-the-proposed-data-accessibility-policy-free-more-data-or-lock-it-up-tighter-behind-legalese-8174951.html>> accessed 16 March 2022

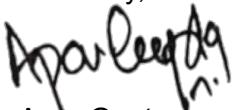
<sup>5</sup> Anushka Jain and Apar Gupta, 'Understanding the Draft India Data Accessibility & Use Policy, 2022' (*The Hindu*, 24 February 2022)

<<https://www.thehindu.com/sci-tech/technology/understanding-the-draft-india-data-accessibility-use-policy-2022/article65077964.ec>> accessed 16 March 2022

<sup>6</sup> 'RTI to the Ministry of Electronics and Information Technology on the Draft Data Accessibility and Use Policy 2022' (*Internet Freedom Foundation*, 8 March 2022) <<https://drive.google.com/file/d/13WMNPNPHCaL0C79WrKDtFlumpyf0hZQx/view>> accessed on 16 March 2022

5. Broadly speaking, certain key concepts of the Draft Data Access Policy have now been removed, which includes its application over personal data, identification of certain data-sets as high value, and pricing & licensing frameworks to enable the sale of these datasets. Through these changes we may infer that MeitY has tried to respond to the public criticism of the Draft Data Access Policy's objectives of commercialisation of citizen data by the Government. However, while these quick fix changes superficially try to incorporate some of the criticism levied towards the Draft Data Access Policy, they fail to resolve the core conceptual criticism with the Draft Data Access Policy.
6. Therefore, our previous comments submitted on March 4, 2022 (IFF/2022/012) still hold ground as the new policy document did not make material changes.<sup>7</sup> Non-personal data has not been defined, leaving the door open to vagueness and arbitrary interpretations. International opinion on such issues has generally strayed towards a more robust definition of NPD. Furthermore, the threat of deanonymisation does not seem to have been adequately accounted for: several studies have shown that certain anonymised datasets have been found to be vulnerable to techniques of de-anonymisation.<sup>8,9</sup>
7. Thus, we believe that this policy must be immediately withdrawn, and that a fresh consultation process should be initiated that ensures transparency as these numerous changes have completely vitiated the ongoing consultation process. Additionally, it would be appropriate to conduct a departmental inquiry into this entire matter.

Sincerely,



Apar Gupta

Executive Director

Internet Freedom Foundation

[apar@internetfreedom.in](mailto:apar@internetfreedom.in)

**Annexure 1:** Copy of IFF's comments on the Draft India Data Accessibility & Use Policy, 2022 dated March 4, 2022

---

<sup>7</sup> 'Comments on Draft India Data Accessibility & Use Policy, 2022' (*Internet Freedom Foundation*, 4 March 2022) <[https://drive.google.com/drive/folders/1juyn5\\_awzLrxD7EDK18gDdaebqDJgeUS](https://drive.google.com/drive/folders/1juyn5_awzLrxD7EDK18gDdaebqDJgeUS)> accessed 16 March 2022

<sup>8</sup> Wei-Han Lee, Changchang Liu, Shouling Ji, Prateek Mittal and Ruby Lee, 'Quantification of De-anonymization Risks in Social Networks' (*Princeton Architecture Laboratory for Multimedia and Security*, March 15 2017) <<http://palms.ee.princeton.edu/system/files/Quantification+of+De-anonymization+Risks+in+Social+Networks.pdf>> accessed 17 March 2022

<sup>9</sup> Sébastien Gambs, Marc-Olivier Killijian, Miguel Núñez del Prado Cortez, 'De-anonymization attack on geolocated data' (*Journal of Computer and System Sciences*, April 18 2014) <<https://www.sciencedirect.com/science/article/pii/S0022000014000683>> accessed 17 March 2022



**INTERNET  
FREEDOM  
FOUNDATION**

[internetfreedom.in](http://internetfreedom.in)

[policy@internetfreedom.in](mailto:policy@internetfreedom.in)

+91 011 4143 7971

**Annexure 2:** Table of Changes made to Draft India Data Accessibility & Use Policy 2022 Document

By Email/ Post

To,  
Shrimati Kavita Bhatia,  
Scientist F,  
Ministry of Electronics and Information Technology  
Electronics Niketan, 6, CGO Complex,  
Lodhi Road, New Delhi - 110003  
Email id: [khatia@gov.in](mailto:khatia@gov.in)  
CC: [pmu.etech@meity.gov.in](mailto:pmu.etech@meity.gov.in)

Dated: March 4, 2022

IFF/2022/012

Dear ma'am,

**Re: Comments on Draft India Data Accessibility & Use Policy, 2022**

1. The Internet Freedom Foundation (“IFF”) is a registered charitable trust which advocates to protect and advance constitutional freedoms in a digital society. We work across a wide spectrum of issues, with expertise in free speech, electronic surveillance, data protection, net neutrality and innovation; we aim to champion privacy protections, digital security, and individual freedoms in the digital age.
2. We are writing to you to offer our inputs on the Draft India Data Accessibility & Use Policy, 2022 (Draft Data Access Policy) on which comments have been invited till March 18, 2022. We commend the objective of the Ministry of Electronics & Information Technology (MeitY) to utilise data to improve the quality of governance and service delivery as well as to promote innovation. We feel that these objectives can only be achieved from a rights centric framework. Ensuring this is vital, as it will ensure that the proposed framework will truly work for the benefit of all individuals.
3. For clarity, our inputs focus on four key clusters:
  - a. Lack of transparency and faulty consultation process.
  - b. Privacy concerns with respect to enhanced data sharing.
  - c. Primary objectives undergirded by perverse economic incentives.
  - d. Ambiguous definitions and the resultant arbitrariness.

I-1718, Chittaranjan Park, New Delhi, Delhi 110019

4. Our principal recommendation here is that MeitY reconsider this policy and aim to withdraw it. We state this with a sense of responsibility after participating in several consultations by MeitY including those concerning the Draft Data Protection Bill, 2021. We have arrived at this recommendation after conducting an extensive study of the Policy. Through this exercise, we have realised that the Policy is based on a faulty objective of revenue generation and fails to sufficiently acknowledge the resultant risks. In our opinion, if enacted, this policy would lead to grave violations of right to privacy and other key user rights such as right to confirmation and access, correction and erasure, data portability and the right to be forgotten. In its present form, it will also facilitate state-sponsored mass surveillance by allowing the creation of 360° profiles of individuals whose data has been collected and processed by government agencies.

We hope MeitY takes forward the specific suggestions made by us.

Sincerely,

Anushka Jain,  
Associate Counsel (Surveillance & Transparency),  
Internet Freedom Foundation.

# **Detailed Submission on Draft India Data Accessibility & Use Policy 2022**



**INTERNET  
FREEDOM  
FOUNDATION**

Internet Freedom Foundation  
I-1718, Third Floor, Chittaranjan Park,  
New Delhi 110019

Internet Freedom Foundation ("IFF") is a registered charitable trust which advocates for the digital rights of Indians. Our mission is to ensure the growth of digitisation with democratic rights guaranteed under the Constitution of India.

**Authors:**

**Anushka Jain** is a lawyer and policy researcher interested in disruptive technologies such as artificial intelligence, facial recognition and machine learning. She works as the Associate Counsel (Surveillance & Transparency) at Internet Freedom Foundation. She has done her LL.M. in Intellectual Property and Technology Law from Centre for Post-Graduate Legal Studies at O.P. Jindal Global University, Sonipat and her B.A. LL.B. from Institute of Law, Nirma University, Ahmedabad.

**Shivangani Misra** is a Capstone Fellow hosted at the Internet Freedom Foundation. She is a final-year master's student at O. P. Jindal Global University.

This work is licensed under the Creative Commons Attribution 4.0 International License.



# **TABLE OF CONTENTS**

## **OUTLINE OF THE PRESENT SUBMISSION**

### **1. LACK OF TRANSPARENCY AND CONSULTATION PROCESS**

### **2. CONCEPTUAL ERRORS IN THE DRAFT DATA ACCESS POLICY**

- 2.1 PRIVACY CONCERN WITH RESPECT TO ENHANCED DATA SHARING
- 2.2 PRIMARY OBJECTIVES UNDERGIRD BY PERVERSE ECONOMIC INCENTIVES
- 2.3 AMBIGUOUS DEFINITIONS AND THE RESULTANT ARBITRARINESS

### **3. TABLE PRESENTING CLAUSE-SPECIFIC COMMENTS**

### **4. RECOMMENDATION**

## Outline of the present submission

Our submission is branched into four broad headings for convenience and consideration. Each section highlights an overarching theme along with our comments and recommendations on the Draft India Data Accessibility & Use Policy 2022 (“Policy”). These are namely,

- Lack of transparency and faulty consultation process.
- Privacy concerns with respect to enhanced data sharing.
- Primary objectives undergirded by perverse economic incentives.
- Ambiguous definitions and the resultant arbitrariness.

The overarching analysis contained under these four heads in the first two sections is succeeded in the third section by specific advice on each Clause of the Policy.

Before we proceed with these issues, we would like to commend the intent towards improving India’s digital economy. As the digitisation drive under the Digital India campaign continues, facilitating stronger data protection and privacy measures is vital, especially after the online push seen during the COVID-19 pandemic. In this regard, focusing on digital rights of citizens while drafting data-related policies is important. However, we reiterate that the primacy of privacy and consent over any other objectives of data collection must be maintained to ensure that the collection and processing of data does not result in harm. Further, to ensure government accountability, transparency mechanisms should be strengthened.

Below we provide our comments and recommendations on the Policy.

### **1. Lack of transparency and faulty consultation process.**

- 1.1. A policy drafted and enacted by the government goes through several stages from inception to conclusion. These stages help articulate the problem, provide granularity and depth on the sticky points, source information and concerns from the relevant stakeholders, and finally draft a solution agreeable to all the parties involved. In this context, a consultation paper issued by the government enables a process that supports this purpose leading to informed decision-making. It helps resolve contentious and complex policy issues in areas where the government is trying to build consensus.

- 1.2. However, in drafting the India Data Accessibility & Use Policy, 2022 (Draft Data Access Policy), the Ministry of Electronics and Technology (MeitY) has entirely skipped the consultative process required for drafting a good policy. By sharing the draft proposal directly, Meity has failed to abide by the provisions of the Pre-Legislative Consultation Policy, 2014 ('consultation policy') which was put in place to promote transparency in law-making.<sup>1</sup> The consultation policy was adopted as earlier only a limited number of Bills were published in a draft form for obtaining insights from the relevant stakeholders. In failing to follow the provisions of the consultation policy, MeitY has resorted to a policymaking process which fails to garner public and civil society participation in areas that affect their fundamental rights.
- 1.3. As per paragraph 2 of the consultation policy, the concerned department/ministry should publish any proposed policy both on the internet and through other means.<sup>2</sup> The publication should include a brief justification for the legislation, essential elements of the proposed legislation, its broad financial implications, and an estimated assessment of the impact of the legislation on the environment, fundamental rights, lives and livelihoods of the concerned/affected people, etc.<sup>3</sup> This document should be kept in the public domain for no less than 30 days.<sup>4</sup> The summary of the feedback or comments received from other stakeholders should also be published on the website of the department.<sup>5</sup> In addition to the publication of the document, the department may also hold consultations with all stakeholders.<sup>6</sup>
- 1.4. Unfortunately, MeitY did not meet any of these established thresholds of the consultation policy. The version uploaded on the website on February 21, 2022 claimed the Policy had been arrived at after consultation with stakeholders, even though the identities of these stakeholders were not revealed.<sup>7</sup> The questions raised by these stakeholders and the subsequent inputs given were not made public. Further, upon receiving

---

<sup>1</sup> Ministry of Law and Justice Legislative Department, *Pre-legislative Consultation Policy (PLCP)* (2014) <<https://legislative.gov.in/sites/default/files/plcp.pdf>>

<sup>2</sup> Ibid

<sup>3</sup> Ibid

<sup>4</sup> Ibid

<sup>5</sup> Ibid

<sup>6</sup> Ibid

<sup>7</sup> Wayback Machine, 'Draft India Data Accessibility & Use Policy 2022- Website version on February 21, 2022' ( 21 February 2022) <<https://web.archive.org/web/20220221100523/https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022>> accessed 2 March 2022

such criticism by civil society members over the lack of transparency in the drafting process, MeitY edited their statement on the website.<sup>8</sup> It now states the ‘clauses will be finalised after getting inputs of stakeholders in the consultation process’. This statement update carried out in a hasty manner also fails to address the transparency and accountability concerns raised. As a result, the consultation process followed by MeitY still remains under a dark cloud.

- 1.5. It is also unknown if the Draft Data Access Policy is a result of the sole effort of MeitY or whether other government departments have also been included in the process. According to best practices, a working group is constituted to build consensus and harmonise interests of various stakeholders. This helps in addressing pain points and maintaining accountability over government actions. However, even a working group seems to not have been established, calling the credibility of this policy formulation process by MeitY under question. Therefore, it remains unclear how the recommendations received in the ongoing consultation process will be evaluated and included in the Draft Data Access Policy as well as whether a further round of counter comments would be carried out before finalisation.
- 1.6. Additionally, another area that merits reconsideration is a larger trend of policy-based administration detached from our constitutional framework. As per the separation of powers envisaged under the Constitution of India, every law is enacted after going through the legislative procedure where a proposal is brought in the form of a Bill before the Parliament to receive approval from both the Houses. However, the Draft Data Access Policy bypassed this parliamentary scrutiny as MeitY formulated the policy without parliamentary discussion.
- 1.7. The policy process adopted by MeitY also sidelines India’s federal structure. The Seventh Schedule to the Indian Constitution defines the structure of the distribution of legislative powers between the Centre and the State. However, the centralised manner of decision-making seen here contravenes the federal structure designed specifically as a safeguard against Centre dominance. The proposal to share data has been rejected by State governments earlier as well, such as when the Department of Food and Public Distribution urged States to share Aadhaar details of National Food Security Act (NFS) beneficiaries with the National Health Authority (NHA).<sup>9</sup> The States reportedly pushed back against this demand

---

<sup>8</sup> Ministry of Electronics and Information Technology, *Draft India Data Accessibility & Use Policy* (February 2022) <<https://www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022>>

<sup>9</sup> Soumyarendra Barik, ‘Told to share ration card & Aadhaar data, states push back’ (*Indian Express*, 13 February, 2022) <<https://indianexpress.com/article/india/told-share-ration-card-aadhaar-data-states-push-back-7769898/>>

due to the security implications of such a data transfer, fearing that the data may be used for political gains.<sup>10</sup> However, ignoring these concerns, it appears that MeitY intends on proceeding ahead with the Draft Data Access Policy.

- 1.8. The authenticity of the data cited in the accompanying 'Background Note' can also be called into question as it has been utilised in the absence of satisfactory referencing which would help in verifying its authenticity (barring the Introduction section).<sup>11</sup> Lastly, unlike other consultation papers, this document issued for the purpose of inviting feedback and inputs, also fails to pose any questions which would have helped in getting more nuanced and granular information, perspectives, and recommendations.
- 1.9. To conclude, our recommendations on the basis of the analysis contained in this section is that the consultation process adopted by MeitY is flawed. The present consultation exercise needs to be withdrawn. Instead, MeitY should publish a consultation paper, as per best practices followed by government departments such as the Telecom Regulatory Authority of India as well as in light of contemporary international practices. The comments received should then be made available online and a counter comments period should commence. These counter comments should be corresponding to the updated policy which contains recommendations from the responses received as well as reasons for accepting the recommendations. Further, the policy consultation process should be made multi-lingual to ensure wider public participation. MeitY should also consider writing to the Departments of Information Technology of various State governments to obviate any federal challenges to the data sharing envisaged under the Draft Data Access Policy. This will help in evolving a consensus given that as per Clause 2 of the Draft Data Access Policy, it aims to "radical(ly) transform" India's ability to harness public sector data that will cause far reaching changes to India's data governance structure.

## **2. Conceptual Errors in the Draft Data Access Policy:** Several fundamental issues emerge from the Draft Data Access Policy that include privacy concerns with respect to enhanced data sharing, perverse economic objectives, and ambiguous definitions and the resultant arbitrariness.

---

<sup>10</sup> Ibid

<sup>11</sup> Ministry of Electronics and Information Technology, *India Data Accessibility and Use Policy: Background Note* (February 2022) <<https://www.meity.gov.in/writereaddata/files/Background%20Note%20for%20India%20Data%20Accessibility%20and%20Use%20Policy.pdf>>

Each of these concerns have been separately analysed below with specific recommendations.

## **2.1. Privacy concerns with respect to enhanced data sharing.**

- 2.1.1. A robust data sharing ecosystem, as envisaged by Clause 8 of the Draft Data Access Policy, goes against the purpose limitation principle of data processing.<sup>12</sup> According to the principle, personal information collected and processed should be relevant to the purpose for which they are processed.<sup>13</sup> The entities collecting the information should use the data only for the intended purpose, and any change in it should be conveyed to the user to obtain their consent.<sup>14</sup> Thus, purpose limitation combined with the data minimisation principle aims to limit the use of data to what is consented to by the user.<sup>15</sup>
- 2.1.2. However, in the absence of a data protection law, clear standards need to be drafted defining the contours of data exchange, sharing and processing of personal data. The Draft Data Access Policy should define authorisation of flow of data and purpose specification, as well as technical guarantees for purpose limitation and access control. As the Supreme Court observed in their decision in the matter of *Justice KS Puttaswamy v. Union of India*,

*"Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state."*<sup>16</sup>

---

<sup>12</sup> Amber Sinha, 'New Approaches to Information Privacy – Revisiting the Purpose Limitation Principle' (*The Centre for Internet and Society*, 13 July 2016) <<https://cis-india.org/internet-governance/blog/digital-policy-portal-july-13-2016-new-approaches-to-information-privacy-revisiting-the-purpose-limitation-principle>>

<sup>13</sup> Ibid

<sup>14</sup> Ibid

<sup>15</sup> 'Principle (c): Data minimisation' (*Information Commissioner's Office*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/#:~:text=What%20is%20the%20data%20minimisation%20principle%3F,-Article%205>>

<sup>16</sup> *Justice K.S.Puttaswamy(Retd) vs Union Of India* [2017] 10 SCC 1

2.1.3. The Draft Data Access Policy may also work against the proposed Data Empowerment and Protection Architecture (DEPA) policy which foregrounds the consent of the user as primary.<sup>17</sup> While DEPA has its own limitations, the policy objective of giving precedence to user consent is commendable. In contrast, the Draft Data Access Policy has skipped consent completely. Instead, the government department harnessing the data will become the ‘owner’ of it, as per Clause 16.2 of the Draft Data Access Policy, and decide how it should be shared with other departments and for how much, essentially making personal data of citizens a saleable commodity.

2.1.4. Such a provision is worrisome, considering that this may enable the building of a 360° profile of every citizen. A 360° profile uses a single ID number across datasets to link together different data sources.<sup>18</sup> The use of unique digital identifiers or even phone numbers, may lead to unauthorised profiling of individuals through correlation of identities across multiple application domains.<sup>19</sup> Therefore, the owner of this dataset will possess a tremendous volume of information about a person, potentially without their knowledge as to the nature of the datasets being used or how the dataset may be utilised. Hence, collection of data by multiple agencies to create such comprehensive profiles of individuals may facilitate greater surveillance, thus impeding the efforts towards recognising privacy as a fundamental right flowing from the right to life & liberty under A.21 of the Constitution of India.

2.1.5. For instance, the Government of India’s Digital India programme envisions the creation of a ‘cradle to grave’ digital identity.<sup>20</sup> In order to provide welfare services effectively, these e-governance schemes collect and store information through the lifecycle of an individual, providing a 360° identification.<sup>21</sup> The schemes under Digital India conceptualise a digital ecosystem, with Aadhaar

---

<sup>17</sup> Niti Aayog, *Data Empowerment and Protection Architecture: Draft for Discussion* (August 2020) <https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf>

<sup>18</sup> Privacy International; *The Sustainable Development Goals, Identity, and Privacy: Does their implementation risk human rights?*; August 29, 2018; <https://privacyinternational.org/long-read/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk>

<sup>19</sup> Subhashis Banerjee & Subodh V. Sharma, ‘Protecting data privacy: Authorisation and access control’ (*Ideas for India*, 4 July, 2018) <https://www.ideasforindia.in/topics/governance/protecting-data-privacy-authorisation-and-access-control.html>

<sup>20</sup> Ministry of Electronics & Information Technology, *Digital India* <<https://www.digitalindia.gov.in/>>

<sup>21</sup> Elonnai Hickok, Sumandro Chattapadhyay & Sunil Abraham, ‘Big Data in Governance in India: Case Studies’ (*The Centre for Internet & Society*, 19 February, 2017) <https://cis-india.org/internet-governance/files/big-data-compilation.pdf>

functioning as the primary form of identity used to enter this ecosystem.

- 2.1.6. Similarly, federated registries of ID constitute one of the core building blocks of the InDEA 2.0 policy.<sup>22</sup> As the world becomes data rich, InDEA 2.0 asserts the importance of various data about people, entities, geographies, resources, assets, etc. being made available in electronic registries with Open APIs for other applications to seamlessly validate and use attested and authenticated data.<sup>23</sup> Federated Digital IDs aims to link an individual's multiple unique IDs such as PAN, Aadhaar, driving licence, passport, etc. to one unique ID for seamless flow of data. This shows that valuable data is often aggregated, group, or anonymised data, posing risks without an enforceable data protection law or authority to monitor and provide legal remedies.
- 2.1.7. Further, legislative concerns arise from the cross-departmental interlinkage of databases. The Supreme Court's ruling in the Privacy judgement and subsequently the Aadhaar decision (*Justice K.S. Puttaswamy (Retd) & Anr v. Union of India & Ors*, 2018) mandate that the use of individuals' personal data and the interlinkage of individuals' databases must satisfy the three-part test set out in the Privacy judgement.<sup>24</sup> To this end, essential service delivery using public data from the government must be carefully calibrated, especially given clear regulatory lines drawn after the Aadhaar decision.
- 2.1.8. Much has been written and said about Aadhaar's weak privacy provisions, which may open the door to unauthorised mass surveillance.<sup>25</sup> Once one's Aadhaar number becomes publicly available, given that it must be necessarily disclosed by beneficiaries, it increases the risk of identification without consent across domains.<sup>26</sup> Moreover, anyone with access to the 'control' end of the Ginger platform may gain access to all the

---

<sup>22</sup> Ministry of Electronics & Information Technology; *InDEA 2.0*; January 2022; [https://www.meity.gov.in/writereaddata/files/InDEA%20\\_0%20Report%20Draft%20V6%202024%20Jan%202022\\_Rev.pdf](https://www.meity.gov.in/writereaddata/files/InDEA%20_0%20Report%20Draft%20V6%202024%20Jan%202022_Rev.pdf)

<sup>23</sup> Ibid

<sup>24</sup> *Justice K.S.Puttaswamy(Retd) vs Union Of India* [2017] 10 SCC 1

<sup>25</sup> Reetika Khera, *The Different Ways in Which Aadhaar Infringes on Privacy*, (*The Wire*, 19 July 19) <<https://thewire.in/government/privacy-aadhaar-supreme-court>>

<sup>26</sup> Shweta Agrawal, Subhashis Banerjee & Subodh Sharma, 'Privacy and Security of Aadhaar: A Computer Science Perspective' (*Computer Science and Engineering, IIT Delhi*) <<https://www.cse.iitd.ac.in/~suban/reports/aadhaar.pdf>>

data associated with an Aadhaar number. Thus, UIDAI effectively gets access to all “seeded” data. Seeding allows multiple databases to be tagged with unique identifiers, thus establishing a relationality as well as enabling big data analytics.

2.1.9. As the Draft Data Access Policy intends on mandating all government departments to ‘comply with the minimum anonymisation standards defined by India Data Office/ MeitY or any statute/act/policy issued by the government of India’, it is concerning that it fails to acknowledge the technical ease with which de-anonymisation of data can be conducted.<sup>27</sup> Several studies have indicated the increased threat of de-anonymisation, both directly and indirectly. Direct attacks through decryption may, for example, “successfully identify users’ Netflix records, uncovering their political preferences and other potentially sensitive information”.<sup>28</sup> Meanwhile, indirect ‘inference’ attacks use already available data “to deduce new personal information not explicitly present in the original data”.<sup>29</sup> The real-world effects of these attacks have already been demonstrated. One study showed that just 4 data points about mobile phone location could uniquely identify 95% of the test population.<sup>30</sup> Another study showed that just three transactions are enough to identify an individual’s credit card.<sup>31</sup>

2.1.10. Additionally, MeitY will depend on anonymisation standards developed by MeitY itself to ensure data protection. There will be no third party checks for quality or effectiveness of the tools deployed, no independent regulator to assess the effectiveness of the anonymisation standards adopted. Essentially, this means the public will have no control over their data once they register with the government. The government will own data of users, process it without their consent and extend no transparent or

---

<sup>27</sup> Ministry of Electronics and Information Technology, *India Data Accessibility and Use Policy (Draft)*, (February 2022) <<https://www.meity.gov.in/writereaddata/files/Draft%20India%20Data%20Accessibility%20and%20Use%20Policy.pdf>>

<sup>28</sup> Wei-Han Lee, Changchang Liu, Shouling Ji, Prateek Mittal, Ruby Lee, ‘Quantification of De-anonymisation Risks in Social Networks’ in Princeton Architecture Laboratory for Multimedia and Security [15 March 2017] <<http://palms.ee.princeton.edu/system/files/Quantification+of+De-anonymisation+Risks+in+Social+Networks.pdf>>

<sup>29</sup> Sébastien Gambsa, Marc-Olivier Killijian, Miguel Núñez del Prado Cortez, ‘De-anonymisation attack on geolocated data’ in Journal of Computer and System Sciences’ [18 April 18 2014] <<https://www.sciencedirect.com/science/article/pii/S0022000014000683>>

<sup>30</sup> Lisa Zyga, ‘Study shows how easy it is to determine someone’s identity with cell phone data’ (*Phys.org*, 25 March 25 2013) <<https://phys.org/news/2013-03-easy-identity-cell.html>>

<sup>31</sup> Jeremy Kirk, ‘How three small credit card transactions could reveal your identity’ (*Computer World*, 25 January 2015) <<https://www.computerworld.com/article/2877935/how-three-small-credit-card-transactions-could-reveal-your-identity.html>>

legal mechanisms for the user to confirm the protection of their data. Hence, this clearly indicates the primary objective of the Draft Data Access Policy to be to serve the economic interests of the government by treating personal data of users as a raw material to be polished for the final sale.

- 2.1.11. The lack of an anchoring legislation to support the Draft Data Access Policy also dilutes its legal standing. Moreover, framing it in the absence of a data protection law, which has its own limitations, also blurs the government's intention on working towards data privacy and protection rights of users. Internationally recognised data protection principles of lawfulness, consent, purpose limitation, data minimisation and accountability have been endorsed by the Supreme Court of India in the Right to Privacy decision. These sentiments, in their entirety, have not been statutorily codified in the Personal Data Protection Bill 2019.<sup>32</sup> The bill, if enacted, in its current form, will not be adequate as it provides multiple exemptions to consent mechanisms for both government agencies and private entities, thus undermining the digital rights of users.
- 2.1.12. The Draft Data Access Policy's monitoring and enforcement provision also creates confusion over who will have the final say in case of a data breach. The proposal says an India Data Office (IDO), constituted by MeitY will be created to monitor the implementation of the Draft Data Access Policy. However, with the data protection bill proposing the creation of a Data Protection Authority (DPA), it is unclear if the IDO will be answerable to the DPA since the latter is designated to be the primary authority regulating data protection norms. The Draft Data Access Policy should lay down clear guidelines on the separation of powers between the IDO and the DPA, and indicate who will have the final word on matters pertaining to public data to prevent future conflicts.
- 2.1.13. The Draft Data Access Policy, in its present form, encroaches upon the privacy rights of Indian citizens. By promoting interdepartmental data sharing in the absence of a data protection law, the Data Access Policy leaves citizens vulnerable to data breaches without due legal recourse. MeitY recommends anonymisation of data to protect against privacy violations;

---

<sup>32</sup> The Personal Data Protection Bill (Bill 373 of 2019) <[http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf)>

however, as we have explained above, de-anonymisation of data can be conducted with ease. Hence, we recommend MeitY to reconsider the Data Access Policy considering the multiple digital right threats the policy may bring. Future data sharing exercises for the purpose of increasing service delivery by the government should only be implemented keeping in mind any privacy concerns that may arise.

## **2.2. Primary objectives undergirded by perverse economic incentives.**

- 2.2.1. It is unfortunate to see that a policy premised on public data is driven by the aim of helping India achieve its ambitious goal of being a \$5 trillion economy. Furthermore, the Background Note accompanying the Draft Data Access Policy document states that emerging technologies are “expected to generate \$1 trillion in economic value for India”.<sup>33</sup> However, this data is based on a Ernst & Young report published in 2019, a time before the COVID-19 pandemic. Hence, these goals have to now be realigned according to present realities.
- 2.2.2. Additionally, based on the preamble as per Clause 1 of the Draft Data Access Policy, this perverse economic objective depends on India’s ability to harness the value of data.<sup>34</sup> The Draft Data Access Policy uses statements like “data is a valuable economic resource”, “data inventories”, and “promote such data sharing”, making personal data of citizens a saleable commodity. This revenue generation or data monetisation objective of MeitY sets a dangerous precedent as it will prompt a financial incentive for state authorities to collect more data than necessary for specific purposes and violate the internationally recognised best practice of purpose limitation in data processing.<sup>35</sup> The profit motive may thus create a troublesome incentive for greater amounts of data collection and retention beyond the purpose consented by users.
- 2.2.3. It appears that the initiative to propose a Draft Data Access Policy stems from the 2018-19 Economic Survey which had a separate chapter titled ‘data “of the people, by the people, for

---

<sup>33</sup> Ministry of Electronics and Technology, ‘*India Data Accessibility and Use Policy: Background Note*’ (February 2022) <<https://www.meity.gov.in/writereaddata/files/Background%20Note%20for%20India%20Data%20Accessibility%20and%20Use%20Policy.pdf>>

<sup>34</sup> Ministry of Electronics and Information Technology, ‘*India Data Accessibility and Use Policy (Draft)*’ (February 2022) <<https://www.meity.gov.in/writereaddata/files/Draft%20India%20Data%20Accessibility%20and%20Use%20Policy.pdf>>

<sup>35</sup> ‘GDPR: Principles relating to processing of personal data’ (*Intersoft Consulting*) <<https://gdpr-info.eu/art-5-gdpr/>>

the people’’.<sup>36</sup> The survey approached data as a ‘public good’ to be harnessed for improving e-governance. It stated that the government will be able to “deliver a better experience to the citizens by bringing disparate datasets scattered across various ministries together”.<sup>37</sup> The Draft Data Access policy has taken this approach ahead with the aim of enhancing access, quality, and use of data to improve delivery of government welfare services. While the intention of increasing the ease of living of citizens through evidence-based policymaking is commendable, it lacks thought towards ensuring the protection of the privacy of citizens. The 2018-19 Economic Survey as well as the Draft Data Access policy have given scant attention to user privacy as well as the security of data. Both have similarly failed to acknowledge the lack of a data protection law in India, without which any policy utilising personal data fails to provide legal remedies to users in case of rights violations.

- 2.2.4. Moreover, the Survey states the high private sector investment in data-related endeavours by citing a Forbes study which found that 53 per cent of companies actively use big data to make decisions.<sup>38</sup> It uses this research to motivate big data usage in government departments. However, the Survey does not acknowledge India’s lack of digital infrastructure and laws to adequately protect the collected data. Responding to a question on cyber crimes related to breach of privacy and fraud posed in the Lok Sabha, Minister of State for Electronics and Information Technology Rajeev Chandrasekhar informed the house that the Indian Computer Emergency Response Team (CERT-In) had reported a total number of 454, 472, 280 and 138 phishing incidents during the year 2018, 2019, 2020, and 2021 (upto June) respectively.<sup>39</sup> In terms of cyber attacks on government organisations, he said CERT-In observed 70,798, 85,797, 54,314 and 12,001 incidents during the year 2018, 2019, 2020 and 2021 (upto June) respectively.<sup>40</sup>

---

<sup>36</sup> Ministry of Finance, ‘Economic Survey 2018-19: Volume 1’ (2018) <[https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/vol1chapter/echap04\\_vol1.pdf](https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/vol1chapter/echap04_vol1.pdf)>

<sup>37</sup> Ibid

<sup>38</sup> Ibid

<sup>39</sup> Government of India, ‘Unstarred Question No. 2633: Increase in Cyber Crimes’ (Lok Sabha, 2021) <<http://164.100.24.220/loksabhaquestions/annex/176/AU2633.pdf>>

<sup>40</sup> Government of India, ‘Unstarred Question No. 2612: Cyber Attack on Organisations’ (Lok Sabha, 2021) <<http://164.100.24.220/loksabhaquestions/annex/176/AU2612.pdf>>

- 2.2.5. Such cybersecurity lapses weigh heavily on the economy as well. A report by IBM Security revealed that the average total cost of a data breach in 2021 was Rs 165 million, a 17.85 per cent increase from 2020.<sup>41</sup> The report also noted that the average time to detect a breach went up from 230 days to 239 days, while the average time to contain a breach went down from 83 to 81 days.<sup>42</sup> This indicates a significant amount of information and data loss for users. Evidence suggests that prior to embarking on a nation-wide campaign to harness data and digitisation, policymakers should first direct resources and time into drafting a comprehensive data protection law. A robust digital infrastructure needs to be built to ensure uniform ability across government sectors to maintain and protect personal data, whilst keeping informational privacy rights of citizens in mind.
- 2.2.6. Further, the pricing and licensing proposal under Clause 11 in the Draft Data Access Policy poses an immediate risk as it makes the government a data broker. While MeitY claims to have introduced the Draft Data Access Policy to increase their transparency and accountability to the public, pricing of datasets will limit the ability to access data to the wealthy, thereby defeating the intended goal. The Draft Data Access Policy states that “to promote innovation and unlock the value potential of data, certain detailed data sets that have undergone value addition/transformation may be valued appropriately”.<sup>43</sup> This makes the pricing decision of data arbitrary as each government department will design their own pricing rules. Moreover, as the purpose of the Draft Data Access Policy is to enable inter-departmental access of data, it is unclear how the final dataset which has gone through various levels of processing and analysis will be priced. The final dataset may include information provided by several government departments, hence; it remains unclear how final valuation will be done.
- 2.2.7. As the Draft Data Access Policy incentivises and promotes data sharing, it may push the government towards collecting more

---

<sup>41</sup> ‘IBM Report: Cost of a Data Breach Hits Record High During Pandemic’ (IBM Newsroom, 28 July 28 2021) <<https://in.newsroom.ibm.com/IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic?lnk=hm>>

<sup>42</sup> Ibid

<sup>43</sup> Ministry of Electronics and Information Technology, ‘India Data Accessibility and Use Policy (Draft)’ (February 2022) <<https://www.meity.gov.in/writereaddata/files/Draft%20India%20Data%20Accessibility%20and%20Use%20Policy.pdf>>

data than necessary. Commercial interests will prompt the government to collect more granular personal details through greater capture of data and increased retention periods. This unrestrained collection of information will risk Indian citizens' government records being sold and profiled by the private sector.

- 2.2.8. The data sharing principle of the Draft Data Access Policy will also contradict the data minimisation principle recognised by the Supreme Court of India in the fundamental right to privacy judgement, *Justice KS Puttaswamy v. Union of India*.<sup>44</sup> As the Draft Data Access Policy propagates incentive-based data collection, state governments may also be tempted to let go of their privacy and security concerns for generating additional revenue. A similar case was seen in 2020 when the Ministry of Road Transport and Highways (MoRTH) withdrew the Bulk Data Sharing Policy following concerns over privacy and misuse of data.<sup>45</sup> The Bulk Data Sharing Policy, formulated in 2019, allowed MoRTH to "share complete data" with specified agencies, automobile industries, banks and finance companies.<sup>46</sup>
- 2.2.9. While this mostly held non-personal details like chassis number, model type, year of manufacture among others, the MoRTH itself admitted that this data could be subject to triangulation. Here, triangulation refers to the combination of different data-sets, which individually do not reveal much but when viewed together lead to individual identification and the dilution of user privacy. This helped the government earn Rs 1,11,38,79,757 over 2019-20, a year wherein the country's fiscal deficit widened to 4.6 per cent of the Gross Domestic Product (GDP).<sup>47,48</sup> Hence, it appears that the Bulk Data Sharing policy proceeded from an

---

<sup>44</sup> *Justice K.S.Puttaswamy(Retd) vs Union Of India* [2017] 10 SCC 1

<sup>45</sup> Shreya Nandi, 'Govt to scrap bulk data sharing policy privacy, misuse concerns' (*Livemint*, 26 June 2020) <<https://www.livemint.com/news/india/govt-to-scrap-bulk-data-sharing-policy-for-vehicles-driving-licences-11593005278063.html>>

<sup>46</sup> Ministry of Road Transport and Highways, 'Bulk Data Sharing Policy & Procedure' (2019) <<https://parivahan.gov.in/parivahan/sites/default/files/NOTIFICATION%26ADVISORY%26March%202019.pdf>>

<sup>47</sup> Government of India, 'Unstarred Question No.1734: Bulk Data Sharing Policy & Procedure' (*Lok Sabha*, 11 February 2021) <<http://164.100.24.220/lok sabha questions/annex/175/AU1734.pdf>>

<sup>48</sup> Harshita Singh, 'Fiscal deficit widens to 4.6% of GDP in 2019-20' (*Hindustan Times*, 29 May 2020) <<https://www.hindustantimes.com/business-news/fiscal-deficit-widens-to-4-6-of-gdp-in-2019-20/story-4fsZTJpYQUw8Me1dWT0UZP.html>>

economic standing ignoring data privacy issues acknowledged a year later.

2.2.10. The Draft Data Access Policy proceeds from an incorrect economic understanding. Clause 1.1 of the Draft Data Access Policy sets a perverse economic foundation by stating ‘data is a valuable economic resource’ offering ‘enormous opportunities’ for businesses and governments. This indicates MeitY’s intention of treating personal data of citizens as a resource to be processed for financial gains. This economic incentive will result in excessive data collection. Implementing the Draft Data Access Policy without a robust cybersecurity infrastructure in place also runs serious risk of online fraud and privacy infringement.

### **2.3. Ambiguous definitions and the resultant arbitrariness.**

2.3.1. Vague provisions suffer from the vice of being susceptible to over-broad and harmful interpretation. The Supreme Court, in its landmark decision in the matter of *Shreya Singhal vs Union of India*, had declared S.66A of the Information Technology Act, 2000 as unconstitutional and void for vagueness.<sup>49</sup> The provision was struck down specifically because its over-broad provisions allowed for arbitrary interpretations which were used to curb free speech on the internet. Several key concepts which have either been introduced or used in the Draft Data Access Policy suffer from a similar vice of vagueness and lack of clarity, or, in some cases, wilful misinterpretation.

2.3.2. Further, important terms have been left to be defined by subsequent frameworks, to be released at a later date. It is unclear whether these subsequent frameworks will be made available for public consultation and feedback. Such practices defeat the purpose of a public consultation exercise as stakeholders responding to the Draft Data Access Policy cannot provide their insight on how key concepts, which shape the nature of the Draft Data Access Policy, have been defined. Our specific concerns with some of the key concepts utilised in the Draft Data Access Policy are:

2.3.2.1. **Data anonymisation:** The definition of ‘data anonymisation’, contained in the Annexure to the accompanying Background Note, has been defined

---

<sup>49</sup> *Shreya Singhal vs U.O.I* [2015] SC 1523

incorrectly as an irreversible process based on certain standards of irreversibility to be specified by the competent authority. For this, “reference anonymisation tools” will be provided as per Clause 13 of the Draft Data Access Policy. There are three broad issues with the data anonymisation provisions in the Draft Data Access Policy. Firstly, according to multiple studies published by cybersecurity researchers, re-identification from anonymised datasets is possible, unless strict access control provisions are put in place.<sup>50,51</sup> Secondly, the anonymisation tools that are going to be provided may not be sufficient to protect against re-identification. It is not known whether these tools will be opened to qualitative scrutiny by independent actors who will be able to verify their effectiveness. Thirdly, the anonymisation standards which have to be complied with under Clause 13 have not been issued, therefore their adequacy and effectiveness can not be determined.

**2.3.2.2. Open by default:** ‘Open by default’ has been indicated as one of the 12 principles on which data sharing and governance under the Draft Data Access Policy need to be based, as per Clause 5. However, in practice MeitY fails to correctly apply the concept of open data. The core principle and objective of the concept of open data is government transparency. However, there is only one mention of transparency and almost no mention of how data sharing, as envisaged under the Draft Data Access Policy, will help fulfil demands for accountability and redress. Instead, the policy incentive behind making data open seems to be maximising revenue generation.

**2.3.2.3. High-Value Data Sets:** Under Clause 10, which relates to ‘High-Value Data Sets’, it has been indicated that access to these data sets will be accelerated. However, the Clause fails to define which datasets will be categorised to be high-value and states that an

---

<sup>50</sup> ‘Anonymising personal data ‘not enough to protect privacy’, shows UCLouvain’s new study’ (*UCLouvain*) <<https://uclouvain.be/en/discover/news/anonymising-personal-data-not-enough-to-protect-privacy-shows-uclouvain-s-new-study.html>>

<sup>51</sup> Luc Rocher, Julien M Hendrickx, Yves-Alexandre de Montjoye, ‘Estimating the success of re-identifications in incomplete datasets using generative models’ [2019] <<https://www.nature.com/articles/s41467-019-10933-3.pdf>>

indicative framework to identify High-Value Data Sets will be notified by the India Data Council eventually. This definition will be on the basis of vague and over-broad terms such as their degree of importance in the market, their degree of socio-economic benefits, their impact on India's Artificial Intelligence strategy and their performance on key global indices. The policy needs to explicitly make clear on what basis this degree of importance and socio-economic benefits be decided to prevent arbitrary decision-making. It has also not been made clear whether this list of terms is exhaustive.

2.3.2.4. **Pricing:** As per Clause 11 of the Draft Data Access Policy, detailed data sets that have undergone value addition/transformation will qualify for monetisation. However, pricing of datasets will be decided by each government department which has developed the dataset. This will lead to datasets being priced arbitrarily as no clear and standard guidelines for pricing of datasets has been prescribed under the Draft Data Access Policy. Under Clause 18, monetisation models would be brought out by MeitY. However, no timeline has been indicated. This makes it difficult for stakeholders to assess the rationale behind the models, thereby hampering transparency and accountability.

2.3.2.5. **Licensing:** Clause 11 of the Draft Data Access Policy also aims to "incentivise data sharing through creative licensing frameworks", however, clear and specific conditions for licensing of datasets have not been laid down. Under Clause 18, licensing frameworks would be brought out by MeitY. However, no timeline has been indicated. This makes it difficult for stakeholders to assess the rationale behind the frameworks, thereby hampering transparency and accountability.

2.3.3. Ambiguity in key provisions of the Draft Data Access Policy will expose it to arbitrary and over-broad interpretations, which may result in harm. Therefore, it is essential that the Draft Data Access Policy be recalled. Further, the absence of clear definitions in the Draft Data Access Policy defeat the purpose of a consultation process as stakeholders will not be able to provide meaningful recommendations.

3. The above sections provide a detailed submission of broad informational privacy and data protection concerns that arise from the Draft Data Access policy. To revise each Clause specifically, below, we present comments corresponding to individual Clauses of the Draft Data Access Policy by trying to take out the intended benefits and foreseeable harms of each Clause individually.

| Clause No. and Title               | Intended Benefit   | Foreseeable Harm  |
|------------------------------------|--|---|
| <b>1. Preamble</b>                 | Data has been identified as an important resource for better governance, service delivery, and innovation in sectors critical for societal transformation. | <ul style="list-style-type: none"> <li>1. Data has been identified as an economic resource to be exploited for achieving economic goals set by the government.</li> <li>2. This will also result in collection of excessive data for the purpose of maximising revenue generation and go against the internationally recognised best practice of data minimisation.</li> </ul>  |
| <b>2. Objectives &amp; Purpose</b> | Recognition of the principles of privacy, transparency, accountability, citizen awareness among others as objectives of the Draft Data Access Policy.      | <ul style="list-style-type: none"> <li>1. The 13 objectives stated under this Clause are not compatible with each other, such as 2.5 which recognises the importance of privacy protection while 2.6 identifies streamlining inter-government data sharing as an objective of the Draft Data Access Policy which would result in privacy violations.</li> <li>2. While the Draft Data Access Policy recognises many beneficial principles as its objectives, the succeeding Clauses fail to put into place provisions that would satisfactorily fulfil these objectives.</li> </ul> |

| <b>Clause No. and Title</b> | <b>Intended Benefit</b> | <b>Foreseeable Harm</b>   |
|-----------------------------|-------------------------|---|
| <b>3. Definitions</b>       | No comment.             | <p>1. The definitions are contained in Annexure-1 of the accompanying Background Note. However, multiple novel concepts which have been introduced in the Draft Data Access Policy that required definitions have not been defined under this Clause. For example: High-Value Data Sets.</p> <p>2. The definitions which are contained in the Clause are incorrect and incomplete. For example: Data anonymisation has been incorrectly defined as an irreversible process and the standards of irreversibility to be followed have not been specified.</p> |

| <b>Clause No. and Title</b> | <b>Intended Benefit</b>  | <b>Foreseeable Harm</b>   |
|-----------------------------|--|---|
| <b>4. Applicability</b>     | No comment.  | <p>1. The Draft Data Access Policy has been applied to all data created/generated/collected/archived by the Government of India or authorised agencies. This may result in violations of the internationally recognised principles of consent and purpose limitation. This is because data may be shared as well as processed in ways which are not congruent with the purpose for which consent from the data principal was obtained.</p> <p>2. While State Governments have been provided with the flexibility to decide whether they want to adopt the provisions of the Draft Data Access Policy, it has not been specified how this freedom will be achieved. This becomes a cause of concern if specific standards are prescribed by the Central government for data sharing, or compliance is made a precondition to financial assistance.</p> |
| <b>5. Principles</b>        | Multiple beneficial principles based on international best practices such as have been included in the Clause. This includes principles such as transparency, user-centred practices & systems, privacy & security by design and well-defined accountability for all stakeholders. | Similar to the Objectives & Purpose Clause, the Draft Data Access Policy recognises many beneficial principles. However, the succeeding Clauses fail to put into place provisions that would satisfactorily fulfil these principles.  |

| <b>Clause No. and Title</b>                     | <b>Intended Benefit</b>   | <b>Foreseeable Harm</b>   |
|---|---|---|
| <b>6. Institutional Framework</b>               | No comment.   | This Clause lays down the framework for operationalisation of the Draft Data Access Policy. Under the Clause, two new offices, that of India Data Office and India Data Council, are to be constituted. The India Data Council will be tasked with defining relevant standards under the Draft Data Access Policy. Such constitution of offices and prescription of standards that may be applicable not only to the Central government but even State governments and schemes administered by them requires legislative deliberation, which is absent. |
| <b>7. Making Data Open by Default</b>           | No comment.   | Under the Clause, all government data has been made open and shareable by default. This violates internationally recognised best practices of consent and purpose limitation for processing of personal data.   |
| <b>8. Government to Government Data Sharing</b> | The Clause aims to minimise duplication of data and enable better delivery of citizen centric services.                                       | We would caution against the consent architecture being proposed through the application of the DEPA framework, as it lacks any legal backing, and thus doesn't provide for any remedies.   |
| <b>9. Integrated Data Portals</b>               | Integration of data portals through APIs will provide administrative benefit and standardise practices of data sharing within the government. | Integration through APIs will facilitate the operationalisation of this flawed policy. Easier access to interdepartmental data would increase the risks of violations of privacy, creation of profiles and enable state-sponsored mass surveillance.  |

| <b>Clause No. and Title</b>     | <b>Intended Benefit</b> | <b>Foreseeable Harm</b>  |
|---------------------------------|-------------------------|--|
| <b>10. High-Value Data Sets</b> | No comment.             | <p>1. The Clause states that some datasets will be identified as high-value and access to them will be accelerated. However, High-Value Data Sets have not been defined under the Draft Data Access Policy, which says that the term will be defined in another framework at a later stage.</p> <p>2. Further, the definition will be on the basis of vague and overbroad terms such as their degree of importance in the market, their degree of socio-economic benefits, their impact on India's Artificial Intelligence strategy and their performance on key global indices. It has also not been made clear whether this list of terms is exhaustive.</p> |

| <b>Clause No. and Title</b>                       | <b>Intended Benefit</b> | <b>Foreseeable Harm</b>  |
|---|-------------------------|--|
| <b>11. Pricing &amp; Licensing</b>                | No comment.             | <p>1. Under the Clause, detailed data sets that have undergone value addition/transformation will qualify for monetisation. However, pricing of datasets will be decided by each government department which has developed the dataset. This will lead to datasets being priced arbitrarily as no clear and standard guidelines for pricing of datasets has been prescribed under the Draft Data Access Policy. Under Clause 18, monetisation models would be brought out by MeitY. However, no timeline has been indicated.</p> <p>2. Similarly, the Clause aims to “incentivise data sharing through creative licensing frameworks”, however, clear and specific conditions for licensing of datasets have not been laid down. Under Clause 18, licensing frameworks would be brought out by MeitY. However, no timeline has been indicated.</p> |
| <b>12. Data Quality &amp; Meta-Data Standards</b> | No comment.             | No comment.  |

| <b>Clause No. and Title</b>                              | <b>Intended Benefit</b> | <b>Foreseeable Harm</b>  |
|--|-------------------------|--|
| <b>13. Data Anonymization &amp; Privacy Preservation</b> | No comment.             | <p>1. Under the Clause, reference anonymisation tools and decision making frameworks will be made available for managing data sharing requests. However, it has not been specified whether these tools will be opened for third party review in order to assess their efficiency. Further, compliance to minimum anonymisation standards has been mandated. However, these standards have not been issued.</p> <p>2. Data sharing has been mandated to take place under existing legal frameworks, policies and legislations of India. However, no such legal framework for protection of privacy has been enacted in India. Further, while compliance to recognised international guidelines has been mandated, other Clauses of the Draft Data Access Policy violate recognised international guidelines of consent, data minimisation and purpose limitation in practice.</p> |
| <b>14. Data Retention</b>                                | No comment.             | The Clause fails to take into consideration the internationally recognised best practice of storage limitation. It states that data should be stored for no longer than is necessary for the purposes for which it was collected to be fulfilled.  |
| <b>15. Capacity &amp; Skill Building Measures</b>        | No comment.             | No comment.  |

| <b>Clause No. and Title</b>                    | <b>Intended Benefit</b> | <b>Foreseeable Harm</b>   |
|--|-------------------------|---|
| <b>16. Data Sharing Toolkit</b>                | No comment.             | Under the Clause, data has been made the property of the government department that generated or collected it. This would seriously undermine the rights of the data principal such as the rights to confirmation and access, correction and erasure, data portability and the right to be forgotten. |
| <b>17. Policy Monitoring &amp; Enforcement</b> | No comment.             | No comment.   |
| <b>18. Implementation Manual</b>               | No comment.             | No comment.   |

4. As can be understood from the detailed analysis above the Draft India Data Accessibility & Use Policy, 2022, has been made available for comments without following the due consultation process which raises transparency concerns. It seems to have been formulated keeping perverse economic objectives in mind without considering citizens' digital rights. Further, the Draft Data Access Policy would lead to serious privacy concerns due to the interdepartmental data sharing structure envisaged under it as well as result in arbitrary application due to inherent vagueness. Therefore, we recommend that MeitY reconsider implementing the Draft Data Access Policy as it has failed to consider the risks that may arise, and aim to recall it.



**INTERNET  
FREEDOM  
FOUNDATION**

Internet Freedom Foundation  
I-1718, Third Floor, Chittaranjan Park,  
New Delhi 110019

Internet Freedom Foundation (“IFF”) is a registered charitable trust which advocates for the digital rights of Indians. Our mission is to ensure the growth of digitisation with democratic rights guaranteed under the Constitution of India.

[internetfreedom.in](http://internetfreedom.in)

**Annexure 2: Table of Changes made to Draft India Data Accessibility & Use Policy 2022 Document**

The table below compares the textual changes made to the Draft India Data Accessibility & Use Policy 2022. It compares the policy document uploaded on the website of the Ministry of Electronics and Information Technology on February 21, 2022 with the version available on March 17, 2022. Any change added or deleted in both the versions of the policy document have been italicised.

| Sr.No | Section in Older Version of Policy Document (February 21, 2022) | Section in Present Version of Policy Document (March 17, 2022) | Older Version of Policy Document (February 21, 2022)   | Present Version of Policy Document (March 17, 2022)  |
|-------|---|--|--|--|
| 1     | Cover Page  | Cover Page   | India Data Accessibility and Use Policy  | India Data Accessibility and Use Policy ( <i>Draft</i> )   |
| 2     | 1.1   | 1.1  | Data is a valuable <i>economic and social</i> resource offering <i>enormous opportunities</i> for citizens, businesses, and governments.   | <i>Non Personal Data</i> is a valuable resource offering <i>better ways of service delivery</i> for citizens, businesses, and governments.   |
| 3     | 1.2   | 1.2  | India's ambitions of becoming a \$5 trillion-dollar digital economy depends on its ability to <i>harness the value of data</i> . Considering this, the India Data Accessibility and Use Policy aims to enhance access, quality, and use of data. | India's ambitions of becoming a \$5 trillion-dollar digital economy depends on its ability to <i>use data for better service delivery</i> . Considering this, the India Data Accessibility and Use Policy aims to enhance access, quality, and use of <i>non-personal data</i> . |



|    |      |      |  |   |
|----|------|------|--|---|
| 4  | 2    | 2    | <i>Such a robust data sharing ecosystem will be unlocked by:</i>   | <i>Objectives of this policy are:</i>   |
| 5  | 2.1  | 2.1  | Maximising access to and use of quality public sector data.  | Maximising access to and use of quality <i>non personal data available with public sector.</i>  |
| 6  | 2.6  | 2.6  | Streamlining inter-government data sharing.  | Streamlining inter-government data sharing <i>while maintaining privacy.</i>  |
| 7  | 2.11 | 2.11 | Enabling secure pathways to share detailed datasets for research & development.  | Enabling secure <i>and privacy compliant</i> pathways to share detailed datasets for research & development.  |
| 8  | 2.12 | 2.12 | Increasing the availability of <i>high-value</i> datasets of national importance.  | Increasing the availability of datasets of national importance.   |
| 9  | 2.13 | 2.13 | Improving overall compliance to data sharing policies and standards.   | Improving overall compliance to data sharing <i>and privacy</i> policies and standards.   |
| 10 | 4.1  | 4.1  | This policy will be applicable to all data and information created/generated/ collected/archived by the Government of India directly or through authorised agencies by various Ministries/ Departments/ Organizations/ Agencies and Autonomous bodies. | This policy will be applicable to all <i>non personal data</i> and information created/generated/ collected/ archived by the Government of India directly or through authorised agencies by various Ministries/ Departments/ Organizations/ Agencies and Autonomous bodies. |



|    |     |     |  |  |
|----|-----|-----|--|--|
| 11 | 5.1 | 5.1 | <i>Open by default</i>   | <i>Identification of datasets for sharing</i>  |
| 12 | 6.1 | 6.1 | India Data Office (IDO) shall be set up by MeitY with an objective to streamline and consolidate data access and sharing of <i>public data</i> repositories across the government and other stakeholders.  | India Data Office (IDO) shall be set up by MeitY with an objective to streamline and consolidate data access and sharing of <i>non personal data</i> repositories across the government and other stakeholders.  |
| 13 | 6.3 | 6.3 | This shall include but not limited to defining frameworks for defining <i>High Value Datasets</i> .  | This shall include but not limited to defining frameworks for defining <i>important Datasets</i> .   |
| 14 | 6.5 | 6.5 | The India Data Office will coordinate closely with line ministries, states and other schematic programs to identify and accelerate access to <i>high value data (HVD)</i> housed with these custodians.  | The India Data Office will coordinate closely with line ministries, states and other schematic programs to identify and accelerate access to <i>non personal datasets</i> housed with these custodians.  |
| 15 | 6.6 | 6.6 | Through the IDO, stakeholders including researchers, start-ups, enterprises, individuals and government departments will be able to access <i>enriched data</i> through mechanisms for data licensing, sharing, and valuation within the overall framework of data security and privacy. | Through the IDO, stakeholders including researchers, start-ups, enterprises, individuals and government departments will be able to access <i>non personal data</i> through mechanisms for data licensing, sharing, and valuation within the overall framework of data security and privacy. |



|    |      |      |  |   |
|----|------|------|--|---|
| 16 | 7    | 7    | <p><i>Making Data Open by Default:</i></p> <p><i>All data for every Government Ministry/ Department/ Organisation shall be open and shareable by default unless:</i></p> <ul style="list-style-type: none"><li><i>- Categorised under the negative list of datasets that won't be shared</i></li><li><i>- Categorised under restricted access and shared only with trusted users - as defined by the concerned Ministry/Department - under a controlled environment.</i></li></ul> | <p><i>Identification of Datasets</i></p> <p><i>Every Government Ministry/ Department/ Organisation shall identify the non-personal datasets available with it and classify them as open, restricted or non-shareable.</i></p> |
| 17 | 10   | 10   | <p><i>High-Value Data Sets</i></p>   | <p><i>Protocols for sharing of non-personal dataset</i></p>   |
| 18 | 10.1 | 10.1 | <p><i>An indicative Framework for identifying High-Value Datasets (HVDs) will be notified by India Data Council. HVDs will be defined based on their degree of importance in the market, degree of socio-economic benefits, impact on India's AI strategy and performance on key global indices.</i></p>   | <p><i>India Data Office will notify protocols for sharing of non-personal datasets. Most datasets shall be made available at no cost to promote innovation and research &amp; development.</i></p>                            |



|    |            |            |  |  |
|----|------------|------------|--|--|
| 19 | 10.2       | 10.2       | <p><i>All government ministries/ departments will adopt the HVD framework to identify, publish and maintain their high-value data sets. MeitY through the IDO will lend advisory support to ministries/ departments to accelerate access to High-Value Datasets.</i></p> | <p><i>Departments/Ministries of Central &amp; State Government organisations and institutions may notify certain datasets for restricted access and define the protocols and processes for access and sharing of such datasets.</i></p>  |
| 20 | No section | 10.3       | No such section  | <p><i>To incentivise and promote such data sharing, innovative and just licensing frameworks that enable fair access and use will be made available by India Data Office which can be used by concerned ministries/ departments.</i></p> |
| 21 | No section | 10.4       | No such section  | <p><i>For restricted access data sharing as per the licensing model adopted, the processes and protocols will be decided by the concerned government department or agency and must be notified in a transparent manner</i></p>           |
| 22 | 11         | No Section | <i>Pricing &amp; Licensing</i>   | No such section  |
| 23 | 11.1       | No section | <i>Minimally processed datasets shall be made available at no cost to promote innovation and research &amp; development.</i>   | No such section  |



|    |      |                 |  |                 |
|----|------|-----------------|--|-----------------|
| 24 | 11.2 | No section      | <p><i>To promote innovation and unlock the value potential of data, certain detailed data sets that have undergone value addition/ transformation may be valued appropriately by the owner</i></p> <p><i>Departments/ Ministries of Central &amp; State Government organisations and institutions.</i></p> | No such section |
| 25 | 11.3 | No such section | <p><i>To incentivise and promote such data sharing, innovative and just licensing frameworks and valuation models that enable fair price discovery will be made available by India Data Office which can be used by concerned ministries/ departments.</i></p>   | No such section |
| 26 | 11.4 | No such section | <p><i>For restricted access data sharing as per the licensing model adopted, pricing of datasets will be decided by the owner government department or agency and must be notified in a transparent manner.</i></p>  |                 |



|    |      |      |   |  |
|----|------|------|---|--|
| 27 | 13.2 | 12.2 | All ministries/ departments must comply with the <i>minimum</i> anonymisation standards defined by IDO/MeitY or by any statute/ act/ policy issued by the government of India.  | All ministries/ departments must comply with the anonymisation standards defined by IDO/MeitY or by any statute/act/policy issued by the government of India.  |
| 28 | 16.2 | 15.2 | Access to data under this policy shall <i>not be in violation</i> of any acts and rules of the government of India in force.  | Access to data under this policy shall <i>be strictly in accordance with</i> any act and rules of the government of India in force.  |
| 29 | 17.2 | 16.2 | India Data Council – <i>comprising of India Data Office and Chief Data Officers of 5 Departments of Government of India – shall be the entity responsible for finalizing Data standards and Metadata standards.</i>   | India Data Council shall be the entity responsible for finalizing Data standards and Metadata standards.   |
| 30 | 18   | 17   | Detailed implementation guidelines including the data sharing toolkit, criteria and mechanism for restricted access data sharing, licensing frameworks and <i>monetisation</i> models would be brought out by the Ministry of Electronics & Information Technology. | Detailed implementation guidelines including the data sharing toolkit, criteria and mechanism for restricted access data sharing, licensing frameworks and <i>sharing</i> models would be brought out by the Ministry of Electronics & Information Technology. |