The Dialogue™
INFORM ENGAGE IDEATE

Comments

OUR RESPONSE TO INDEA 2.0

Authors: Eshani Vaidya, Kamesh Shekar, Saksham Malik **Editors:** Sreyan Chatterjee, Karthik Venkatesh
Research Support: Srija Gadamsetti

ABOUT THE DIALOGUE

The Dialogue is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue was ranked amongst the Top-Ten think-tanks in the world to watch out for by the Think-Tank Civil Societies Programme, Lauder Institute, University of Pennsylvania, in their 2020 and 2021 ranking index.

 info@thedialogue.co

 www.thedialogue.co

TABLE OF CONTENTS

KEY RECOMMENDATIONS

InDEA 2.0 Reference Excerpts	Recommendations
Theme: Architectural Clarity	
2.1.4. Open, Open and Open Design of the digital systems to be built on open source and, to be published as open-source, source, and to conform to open standards. Exceptions shall be justified. Open-Source Software (OSS) has been defined under the Policy on Adoption of Open Source Software for the Government of India to include the right to redistribute and modify open- source code. However, the inclusion of these user rights has not been made mandatory.	• Clearly lay down the manner in which the usage rights associated with each design will be determined, i.e. uniform standards that must be adhered to or freedoms to be provided based on individual licensing agreements.
2.1.4. Open, Open and Open Adopting Open Source Software (OSS), in the existing regulatory regime, poses several compliance hurdles for small and medium enterprises. Larger companies are software agnostic, i.e. are not affected by their software being open/closed sourced.[1]	• The government must engage with more SMEs companies that can provide access to servers without the risk of vendor lock-ins.[2] • The government must explore the adoption of legacy systems, such as GitHub or GiHab385 that already have a large user base in India, rather than developing open databases like OpenForge that are riddled with issues like a complex user interface, broken web-links and poor community management.[3]
2.1.2. Building Block Approach Architect and design systems and ecosystems in terms of minimal and reusable Building Blocks. The core building blocks infuse reusability and interoperability into the InDEA 2.0.	• Update to better protocols that secure the channel between the Relying Party (RP) and Identity Provider (IdP) on top of existing in-browser communication channels can help avoid vulnerabilities in the system.[4]

[1]Civic Data Lab, The State of Free and Open Software in India,Omidyar Network India, Retrieved on 22 February, 2022 from https://state-of-foss.in/the-state-of-foss-report.pdf.
[2]Civic Data Lab, The State of Free and Open Software in India, Omidyar Network India, Retrieved on 22 February, 2022 from https://state-of-foss.in/the-state-of-foss-report.pdf.
[3]Civic Data Lab, The State of Free and Open Software in India, Omidyar Network India, Retrieved on 22 February, 2022 from https://state-of-foss.in/the-state-of-foss-report.pdf.
[4]Cao, Yinzhi et al. (2014). Protecting Web-based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel. RAID 2014: Research in Attacks, Intrusions and Defenses: 276-298.

	• Enabling a two-step authentication approach with Single Sign On's (SSOs) which can reduce the risk of phishing attacks but will not mitigate it.[5]
5.2.4. Verifiable Credentials (VC) Establishing a system of standardized VC documents enables an individual to easily share credentials in a trusted manner anywhere and thereby open up possibilities to access various opportunities and services.	• Blockchain: Storage of VCs on blockchain will decentralize the process by storing data in multiple places simultaneously. Data that is stored on the blockchain network also cannot be manipulated or accessed without other actors noticing it.[6]
2.2.1. Federated Architecture Adopt a federated architecture model for designing digital ecosystems – especially data and applications.	• Terminologies like 'federated structure', 'open data', 'data access' must be expressly defined.
2.2.1. Single Source of Truth Build around the constructs of Single-Source-of-Truth and System-of-Records.	• While this repository of data can act as a single source of truth, it is also essential to have a mechanism to cross-check and evaluate the integrity, cleanliness of the data, as state and non-state actors would use this for critical interventions. For instance, institutionalising periodic audits for both data collection methods and data could help in cross-check. • Comparing the data with an alternative database can also help determine gaps and mistakes in data points within the integrated repository. • The framework should acknowledge that Federated Digital ID created through the integration of repositories can be used for authentication while accepting alternative legal IDs for the same purpose.
2.1.3. Open API-based Prioritise the use of open protocols in the framework, instead of a platform model to ensure healthy competition in the market.	• Competition law issues can arise despite the implementation of open protocol frameworks. As seen in the United Payment Interface (UPI) framework, the manner in which one builds their application atop the open-API can determine whether or not they acquire a dominant position in the market.

[5]Scott, Charles et al. (2016). Examining the Privacy of Login Credentials Using Web-Based Single Sign-On: Are We Giving up Security and Privacy for Convenience?. 2016 Cybersecurity Symposium. Retrieved February 25, 2022.
[6]Reiger, Alexander. (2021). The privacy challenge in the race for digital vaccine certificates. Med 2: 633-634. Retrieved February 24, 2022, from https://orbilu.uni.lu/bitstream/10993/48314/1/PIIS2666634021001677.pdf.

	• Therefore, in addition to developing open protocols, the government must also look into additional safeguards against abuse of dominance.
Theme: Insufficient Legislative Backing	
Robust Data Protection Regime 2.1.7. Data sharing policies appropriate to various sectors shall be notified by the central and state governments, ensuring data protection requirements at the same time. 2.4.4 Lay down clear data sharing policies specific to the relevant domain(s), that enable and regulate the sharing of data, in conformance with the applicable data protection regulations. In the absence of a data protection regime governing and protecting personal data; insufficient infrastructure and systems to share data smoothly across stakeholders; and multiple data protection regulations, it is likely that data remains unregulated. 4.3.1 Under the federated architecture approach of InDEA 2.0, it is important to create a "federated set of registries … All such registries should have their own "digital ID" internally to uniquely identify a record.	• Work in collaboration with sectoral regulators enacting data protection regulation so as to avoid conflict. • Implement data governance policies and regulations in a phased manner to ensure data protection and practices surrounding data sharing are in place to support an open ecosystem. • The framework must lay out the privacy and data protection guidelines for the federated digital ID. • The federated digital ID should have statutory protection and be issued through legislation.
Theme: Ambiguity	
6.1 Enable, don't build InDEA 2.0. emphasizes the principle of 'enable, don't build' but does not provide enough information on the integration of legacy data systems at the state level.	• Integrate successful legacy systems, such as state-level data registries to ensure the maintenance of accurate and updated datasets and make use of existing capabilities. This is in line with the principle of 'enable, don't build.' • The Health Management Information System, 2008, for instance, is used to grade health facilities, review State Programme Implementation plans etc. The data and operational processes can be integrated into the registries maintained under ABDM.
2.1.7. Innovation Data is the oxygen for innovation. Data sharing policies appropriate to various sectors shall be notified by the central and state governments, ensuring data protection requirements at the same time.	• Terminologies like 'federated structure', 'open data', 'data access' must expressly be defined.

While the framework talks about 'federated structure' and 'open data', these terminologies stand vague, bringing in questions like do states have access to data repository including central data and data of other states? Does 'open' here means only for businesses and central government departments? Do source codes remain closed like in the case of Aadhaar architecture, while stakeholders can build over it?	
4.2.5 Federated Registries Many registries are stand-alone while some get interlinked via registry IDs depending on the policies that allow such linking. But, when it comes to delivery of benefits, in addition to usage of Aadhaar, interlinked registries within a state may be required to provide a unified view of benefits delivery.	• The InDEA 2.0 needs to adopt a calibrated safety and data protection approach towards the federated registries. • It must consider adopting a federated learning approach to let processing run on decentralised data located in different servers. • It must mechanise a process through which individuals can track the data flow across the federated registries by creating a dashboard. • The dashboard must empower individuals to manually create the policies and implement conditions according to the data context such that processing and sharing of their inter-linked data remains tied to user control.
2.4.4. Data sharing Lay down clear data sharing policies specific to the relevant domain(s), that enable and regulate the sharing of data, in conformance with the applicable data protection regulations.	• The framework must bring harmonisation by weeding out the overlapping and conflicting scopes and bring them to congruence with other existing policies. • A high-level coordination mechanism comprising various levels of government and relevant departments, ministries etc., must be instituted to enforce data sharing and integration in a coordinated way.

THEMATIC RATIONALE FOR RESPONSES

I. Open Platforms

Define Open Source Software

The emphasis on 'openness' within digital spaces in India goes back several years. The National Policy on Information Technology, 2012, emphasised the need to adopt open standards and promote open source and open technologies. The 'Policy on Adoption of Open Source Software for Government of India' defines open software as 'free and open', i.e. guarantees the right to modify and redistribute the source code in addition to viewing the source code. This conforms with the definition of 'free software' as provided by the Free Software Foundation, which protects users' essential freedoms to 'run, copy, distribute, study, change and improve the source code' available to them.[7]

InDEA 2.0 has focussed on openness in design as one of its core principles. The digital system is meant to be 'built on open source, to be published as open-source, and to conform to open standards'.[8] It is important to define 'openness' within open-source software. The ethos of open software simply guarantees visibility and accessibility to the source code, but often restricts user freedoms by way of licenses or other practices.[9] Users are not always permitted to redistribute copies of the original or modified software.

While access to the source code would be in adherence to the principle of 'transparency', it is likely that without the right to modify and/or redistribute the source code, the 'openness' will stifle innovation. Free access to the source code will allow for the creation of more dynamic and inclusive systems, as users will have the right to amend the code to function in a more efficient manner. Certain publicly developed applications only publish part of the source code, while keeping the server-side of the code hidden. Additionally, the source code published is often an older version of the application that is available on mobile app stores. Without access to the latest, consumable version of the source code, the effectiveness of any modifications made to the code will be diluted. While such a move would reflect transparency, in theory, it would not have any tangible outcomes.

InDEA 2.0 reiterates the governments' commitment to adopt OSS as understood in the Policy on Adoption of Open Source Software for the Government of India. However, neither document issues a 'mandate' to adopt OSS. In the absence of adequate legislative backing, it is likely that several may choose not to adopt OSS. The InDEA 2.0. also allows service providers to provide 'adequate justification' in case they wish to operate in a closed-door system. However, these exceptions have not been expressly laid down. Ambiguity in this regard is dangerous as it may lead to unintended consequences of vendor lock-ins, built-in monopolies and may pose an overall hindrance to innovation. For instance, certain publicly developed applications only publish part of the source code, while keeping the server-side of the code hidden. Additionally, the source code published is often an older version of the application that is available on mobile application stores.

It is important to provide a clear definition of 'open software systems' that provides for the rights of users. It is essential to ensure that such software does not create undue restrictions and hinder the realisation of the potential of an open platform.

[7]Free Software Foundation, What is Free Software?, GNU Operating System, Retrieved on 22 February, 2022 from https://www.gnu.org/philosophy/open-source-misses-the-point.html.
[8]Cl. 2.1.4., InDEA 2.0., Ministry of Communication & Information Technology, 2022.
[3]R. Stallman, Why Open Source Misses the Point of Free Software, GNU Operating System, Retrieved on 23 February, 2022 from https://www.gnu.org/philosophy/open-source-misses-the-point.html.

Recommendations

- Clearly lay down how the usage rights associated with each design will be determined, i.e. uniform standards that must be adhered to or freedoms to be provided based on individual licensing agreements.
- Create a requirement to adopt open software through a legislative mandate.

Business and Community

The uptake of FOSS has been relatively slow in Indian markets because of the lack of strategy and knowledge and capacity around FOSS values and their advantages. Another reason for this is that larger companies are often software agnostic.[10] They remain unaffected by whether their systems are open or closed. However, small, and medium enterprises (SMEs) are hindered by various systemic issues. These include an overall absence of free-software-driven culture and the lack of knowledge and overall belief that FOSS is not a viable business option. Larger companies often do not emphasise adopting FOSS within company systems. This marks a larger issue of the absence of a culture developed around open software.

As highlighted in the InDEA 2.0., training and education will play a significant role in maintaining accurate data and developing smoother processes. Additionally, developing a FOSS is fairly challenging. It requires the consistent efforts of community managers and the creator. While proprietary software may create superior tools due to the large vendor investments, the collaborative and dynamic nature of FOSS may yield better software tools in the long term. Adoption of FOSS does not require as much monetary investment and, with policy-based incentives, can incentivise the development of SMEs. The low cost of setting up enterprises may likely help them incentivise customers to migrate from proprietary closed software to mature FOSS alternatives and provide users with all the support they need.[11]

It is important to ensure that capacity building activities are carried out across various sizes of businesses.[12] Collaboration with the community is also an opportunity to ensure that there are continuous feedback mechanisms and people can appropriately engage with OSS-based technology.

The InDEA 2.0, therefore, must focus on creating an enabling regulatory environment, that builds upon but goes beyond regulatory sandboxes and competency building.

Recommendations

- The government must engage with more SMEs that can provide access to servers without the risk of vendor lock-ins.[13]

[10]Civic Data Lab, The State of Free and Open Software in India, Omidyar Network India, Retrieved on 22 February, 2022 from https://state-of-foss.in/the-state-of-foss-report.pdf.
[11]Civic Data Lab, The State of Free and Open Software in India, Omidyar Network India, Retrieved on 22 February, 2022 from https://state-of-foss.in/the-state-of-foss-report.pdf.
[12]Civic Data Lab, The State of Free and Open Software in India, Omidyar Network India, Retrieved on 22 February, 2022 from https://state-of-foss.in/the-state-of-foss-report.pdf.
[8]Civic Data Lab, The State of Free and Open Software in India, Omidyar Network India, Retrieved on 22 February, 2022 from https://state-of-foss.in/the-state-of-foss-report.pdf.

- Capacity-building activities should also be inclusive and in collaboration with communities to maintain an open channel of communication and develop an OSS value-system among stakeholders.

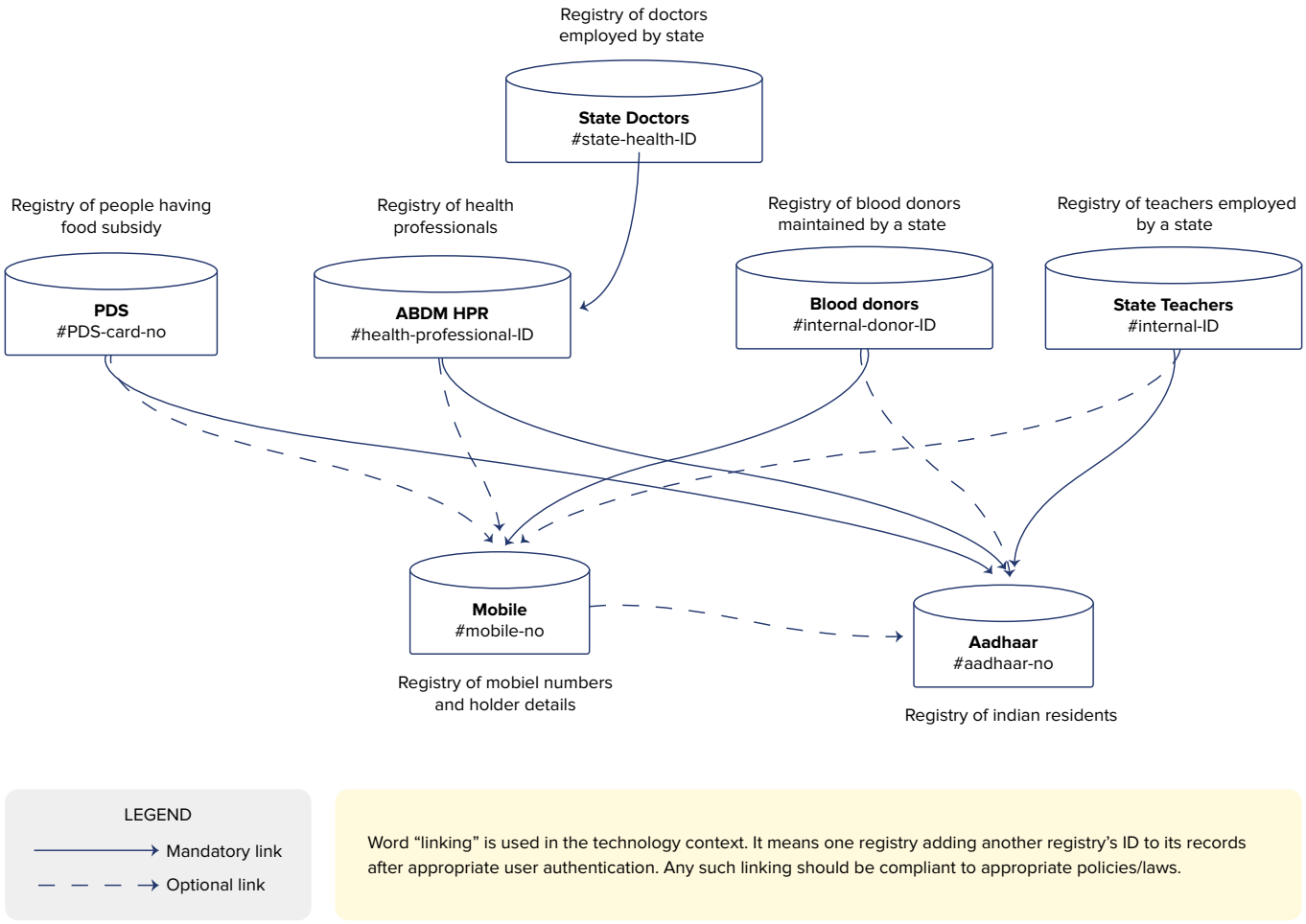
- The government must explore the adoption of legacy systems, such as GitHub or GiHab385 that already have a large user base in India, rather than developing open databases like OpenForge that are riddled with issues like a complex user interface, broken web-links and poor community management.[14]

II. Federated Identities

Interlinkage of Multiple Digital Identities

The InDEA 2.0 provides a framework for maintaining registries and repositories while empowering the user to create, read, update and delete their data. The emphasis on consent managers is a welcome step towards digital ID management. The following Fig. 1 from the document of the InDEA 2.0 shows the possibility of high-level linkages between repositories:

Figure 1. Illustrative Example of Federated Registries



Source: InDEA 2.0, MeitY[15]

[14]Civic Data Lab, The State of Free and Open Software in India, Omidyar Network India, Retrieved on 22 February, 2022 from https://state-of-foss.in/the-state-of-foss-report.pdf.

[15]Ministry of Electronics and Information Technology (MeitY), (2022, January). India Digital Ecosystem Architecture 2.0, Draft for Consultation (Ver 1.0 Jan 22), Retrieved February 24, 2022, from https://www.meity.gov.in/writereaddata/files/InDEA%202_0%20Report%20Draft%20V6%2024%20Jan%2022_Rev.pdf at Pg. 42.

Interlinking various repositories, which include individuals user-controlled and state-controlled id's, may create a system susceptible to cyber attacks. It is likely that, if gained access to, the interlinked registries will allow access to a 360-degree view of the citizen. This would violate an individuals fundamental right to privacy. With several individual id's also linked to foundational identifiers containing biometric data, there is a greater risk to individual privacy. The dangers of violation of the right to privacy will be more significant for the minority and marginalised communities.

In the absence of a data protection regime and surveillance regulation, it is important to examine the power asymmetry between the citizen and the state. Misuse of the data collected or unintended use of the data by business entities or the state could only deepen this divide. In order to effectively secure the citizens right to privacy, the InDEA 2.0 framework should also ensure that the scopes of these exploitative relationships are checked out by imposing optimal liability on the stakeholders.

The InDEA 2.0 does not provide for adequate use cases detailing the manner in which data can be accessed and the purpose of collecting data. In furtherance of an individuals right to informational privacy, it is important to attempt to bridge the information gap and ensure that citizens can effectively exercise their agency. Data empowerment cannot take place while citizens are only provided access to limited information. In most cases, individuals are unaware of the data integration and profiling they are subjected to within these digital systems, which violates their right to privacy.[16]

In conclusion, the envisioned federated identities might lead to negative externalities pertaining to data privacy, security breach, and increased surveillance. We recommend that appropriate mechanisms to prevent the same need to be established before the start of this project.

Recommendations

- Ensure that data protection laws and surveillance reforms are in place prior to adopting federated identities
- Provisions for regular auditing by independent authorities to ensure technical aspects of Federated Identities abide by the legal framework in place.
- The data access and stipulated purpose check mechanism must be instituted as part of InDEA 2.0 to weed out misuse.

Federated registries and Privacy Concerns

The InDEA 2.0 propose interlinking the registries by allowing one registry to add another registry's id to its records (if the policies permit such linking). While we discussed the surveillance concern with federated registries, we want to caution the privacy and data security concerns with interlinking registries.

Figure 1 in this report sourced from InDEA 2.0 document implies that various data registries (mandatory and optional) are ultimately linked to the Aadhaar database. This increases the impact caused by the data breach, which has real life implications, adversely costing individuals and other stakeholders. For instance, Norton reports that about 59% of Indian adults, i.e., 27 million individuals are victims of online identity theft.[17] These

[16]Sethi, Aman. (2018, April 25). Aadhaar Seeding Fiasco: How To Geo-Locate By Caste and Religion In Andhra Pradesh With One Click. HuffPost. Retrieved February 24, 2022, from https://www.huffpost.com/archive/in/entry/aadhaar-seeding-fiasco-how-to-geo-locate-every-minority-family-in-ap-with-one-click_a_23419643.

[17]*Norton survey reveals 59% Indians have dealt with cybercrime in past 12 months.* (2021, April 19). The Indian Express. Retrieved March 8, 2022, from https://indianexpress.com/article/technology/tech-news-technology/norton-survey-reveals-59-indians-have-dealt-with-cyber-crime-in-past-12-months-7280071/

kinds of threats could get exuberated with federated registries and a federated digital id system. The level of impact caused by data breach correlates to some of the factors like:

Nature of the data (sensitivity): Some of the datasets linked through InDEA 2.0 involve sensitive information like health data, financial data etc. If personal data (record) is compromised from one registry, it will also affect the other registries, causing an adverse impact on individuals and society.

Quantity of the data: As InDEA 2.0 envisions interlinking registries, the database increases horizontally (in terms of size) and vertically (in terms of various data points), providing a 360-degree view of individuals and communities. While this would unlock various benefits, in terms of a data breach, the degree of data comprised enticing malicious actors could cause adverse harm.

Connectedness of various stakeholders: While a data breach, in general, can affect individuals and other stakeholders, the data breach of the interlinked database can have an excessive impact as multiple entities across sectors can get affected due to the registry's vastness. Besides, as this registry will be interconnected and available to various stakeholders, it would be difficult to track the data provenance, in turn making tracing the origin of the data breach difficult.

While InDEA 2.0 talks about consent mechanism, from a consumer perspective, with federated registries, individuals lose control over data at transit (when shared or interlinked between various registries), which creates a lack of consumer choice and opacity in treating and transferring sensitive data like payments, medical history, etc.

Recommendations

- InDEA 2.0 talks about privacy-by-design and data security as part of its principles and compliance with data protection regulation. **But, according to the impact, the InDEA 2.0 needs to adopt a calibrated safety and data protection approach toward the federated registries.** The impact must be analysed at various levels of federation based on the three factors discussed above, i.e., nature of data, the quantity of data and connectedness of various stakeholders.

- Rather than interlinking registries for maximising utility, **the InDEA 2.0 must consider adopting a federated learning approach to let processing run on decentralised data located on different servers.** The data must be analysed/used at the respective registries without aggregating/interlinking it into one registry to gain collective inference. This solution paves the way for the decentralisation of data (one of the objectives of InDEA 2.0) without comprising the objective of processing data but reducing the risk of a data breach.

- **InDEA 2.0 must mechanise a process through which individuals can track the data flow across the federated registries by creating a dashboard**. In addition, the envisioned consent mechanism as part of the InDEA 2.0 framework must be enhanced so that **individuals can restrict the flow of data by navigating via the dashboard**. Besides, the dashboard must empower **individuals to manually create the policies and implement conditions** according to the data context such that processing and sharing of their inter-linked data remains tied to user control. The policies can be context-specific such that the same data could have different policies at different registries and levels of federated structure.

Federated Digital ID and Data Protection

The framework layout privacy and data security as some of the key principles. While these principles apply to the data stored in registries, there is less clarity on its applicability to the federated digital ID – a key to the repositories.

Moreover, the federated digital ID will be developed through the INDEA 2.0 framework envisioned by the government without statutory backing. This would make the federated digital ID fall outside the ambit of the upcoming data protection bill, as the definition of one of the sensitive data, i.e., official identifiers".[18]

Recommendations

- The framework must lay out the privacy and data protection guidelines for the federated digital ID.
- The federated digital ID should have statutory protection and be issued through legislation.

SSOs and their Vulnerabilities

Single Sign-Ons (SSOs) have been popular with private entities for years now. In recent years, many Government systems have used SSOs internally to enable secure authentication and access to multiple applications. While Single Sign-Ons are secure, it is important to note that they are not immune to attacks from hacking groups. Recent studies show that 6.5% of investigated relying parties using SSO protocols were vulnerable to impersonation attacks.[19]

Apple, in early 2020, had a design issue with its Single Sign-On feature of 'Sign in with Apple', which enabled users to sign in to third-party applications using their Apple id. The design feature exposed users to the risk of data leakage [20] and was fixed after the security loophole was caught through a bug bounty program by the company.[21]

A months-long nation-state attack in 2020 in the United States of America compromised around 100 companies and a dozen Government agencies.[22] Termed as the 'SolarWinds cyberattack', it reveals the vulnerabilities that a Government system is exposed to due to negligence by third-party cybersecurity partners or collaborators. One of the vulnerabilities that provided entry points for this months-long cyberattack was the SAML/SSO token that SolarWinds' Orion software used for authentication - where a token of highest privileges was replicable by the hackers.[23]

[18]"official identifier" means any number, code, or other identifier, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal.
[19]Cao, Yinzhi *et al*. (2014). Protecting Web-based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel. RAID 2014: Research in Attacks, Intrusions and Defenses: 276-298. Retrieved February 25, 2022.
[20]Data leakage is the unauthorised movement of data from inside the organisation to outside of it.
[21]Phadnis, Shilpa. (2020, June 2). Indian finds bug in Apple, gets Rs 75 lakh. The Times of India. Retrieved February 25, 2022, from https://timesofindia.indiatimes.com/business/india-business/indian-finds-bug-in-apple-gets-rs-75-lakh/articleshow/76146312.cms.
[22]Temple-Raston, Dina. (2021, April 16). A 'Worst Nightmare' Cyberattack: The Untold Story of The SolarWinds Hack. NPR. Retrieved February 25, 2022, from https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.
[23]Microsoft Security Response Center. (2020, December 13). Customer Guidance on Recent Nation-State Cyber Attacks. Retrieved February 25, 2022, from https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/.

SSOs, like any technology, are vulnerable to security risks. Research suggests that SSOs could potentially expose the user to phishing attacks and covert redirections.[24] Using SSOs, not just internally within the Government, but to provide access to users to their data across multiple repositories, hence, increases the surface area of attack.

Recommendations

- Better Protocols: Updating to better protocols that secure the channel between the Relying Party (RP) and Identity Provider (IdP) on top of existing in-browser communication channels can help avoid vulnerabilities in the system.[25]

- Enabling two-step authentication approach with SSOs which can reduce the risk of phishing attacks but does not mitigate it.[26]

Consent and Consent Managers in an Ecosystem of Reusability

Consent is the guiding principle for InDEA 2.0 and is a recurring theme that the framework builds upon. For any privacy-centric framework, users must remain in control of their data, and data is shared and processed *only* in cases where informed and meaningful consent can be obtained.

While reusing the data for various purposes will prevent wastage of time, manpower, and other Government resources;[27] it also raises questions about the consent processes surrounding data collection. Will the user be asked for consent every time a new building block accesses the data? Will the user be asked for consent to use their data in every new project? These questions need urgent answers as they directly relate to users' privacy rights.

The InDEA 2.0 framework provides for the management of data control through consent managers. Other avenues explored include that of Open Data APIs providing the network support instead of a consent manager.[28] It is important to note that data empowerment is different from consent management, and they are not exact substitutes for each other. Data empowerment gives users control over what data is present in the database. Consent management gives users the power over how this data is used. The Data Empowerment and Protection Architecture (DEPA) has been designed to enable the secure sharing of data. One of its guiding principles is that 'individuals have the right to collect, share and access data pertaining to them in an accessible and easily understandable manner'. Building on the objective of the DEPA, it is important to bear in mind that while consent managers are an important first step in securing data empowerment, it is only the first step. It must be followed up with open feedback mechanisms and further collaboration with stakeholders to develop effective means to ensure citizens can meaningfully exercise their agency.

[24]Scott, Charles *et al*. (2016). Examining the Privacy of Login Credentials Using Web-Based Single Sign-On: Are We Giving up Security and Privacy for Convenience?. 2016 Cybersecurity Symposium. Retrieved February 25, 2022.
[25]Cao, Yinzhi *et al*. (2014). Protecting Web-based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel. RAID 2014: Research in Attacks, Intrusions and Defenses: 276-298
[26]Scott, Charles *et al*. (2016). Examining the Privacy of Login Credentials Using Web-Based Single Sign-On: Are We Giving up Security and Privacy for Convenience?. 2016 Cybersecurity Symposium. Retrieved February 25, 2022.
[27]Estonia saves 2% of their GDP annually because of digitised public services and over 1400 years of working time. PWC. Estonia - the Digital Republic Secured by Blockchain. Retrieved February 25, 2022, from https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf
[28]Ministry of Electronics and Information Technology (MeitY), (2022, January). India Digital Ecosystem Architecture 2.0, Draft for Consultation (Ver 1.0 Jan 22), Retrieved February 24, 2022, from https://www.meity.gov.in/writereaddata/files/InDEA%202_0%20Report%20Draft%20V6%2024%20Jan%2022_Rev.pdf at Pg. 50.
[29]NITI Aayog, (2020, August), Data Empowerment and Protection Architecture: Draft for Discussion, Retrieved 1 March 2022, from https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf

Recommendations

- Create a robust content manager mechanism that has to be in place before data is collected from the user. Avoid centralised regulation of all consent managers, and instead build sector-specific capacity and expertise.[30]

- Users must be informed in case the context of processing data was altered. A fresh consent mechanism must be initiated.

Verifiable Credentials

Credentials, such as a driver's license, an Aadhaar number or a degree certificate, constitute our daily lives. A system of Verifiable Credentials (VCs) is one that is cryptographically secure, privacy-respecting and machine-verifiable. The InDEA 2.0. envisages a VC system that contains credential data, metadata and digital signatures.

In order to develop a privacy-respecting VC system, there must be no aggregation of information. Adopting decentralised storage mechanism is unlikely to mitigate the potential harm caused by aggregation of information or correlation. While techniques such as zero-knowledge proofs have been introduced to mitigate these risks, it is still in the nascent stages of development. Additionally, some systems require an intentional correlation of user data. For instance, issuing prescription drugs will likely use correlated data in order to ensure people aren't getting multiple prescriptions of controlled substances. However, deliberate interlinkages must be also assessed.

It is also important to ensure that unintended or unexpected correlations do not take place from the 'presentation' of credentials within the VC system. The presentation of credentials is the packaging of the VC in such a manner that the 'authorship' of data is verifiable.[32] The presentation of credentials often takes place from multiple VCs, with the components of metadata, the credential itself and the proofs, that are often in the form of digital signatures.[33]

The InDEA 2.0 document provides the Co-WIN platform as an example of successful vaccine credentialing in India. Upon observing the precedent set by this VC, there are two key issues that arise:

Storage of the vaccine credentials.

There is a lack of information in the public domain about privacy and storage of data surrounding vaccines in India.[34] Health data regulators have stated that in order to prevent attacks on the facility, they are not revealing where the vaccine credentials are stored.[35] This model primarily violates the 'Avoid Security-by-Obscurity' principle stated under Section 2.4.7 of the InDEA 2.0 document and sets a counterproductive precedent for the future of VCs.

[30]She Dialogue, (2020) Exerpts from Stakeholder Interviews: Digital Health (*transcript will be shared upon request*).
[31]Working Group, Verifiable Credentials Data Model v1.1., World Wide Web Consortium, Retrieved on 1 March 2022 from https://www.w3.org/TR/vc-data-model/#data-first-approaches.
[32]Working Group, Verifiable Credentials Data Model v1.1., World Wide Web Consortium, Retrieved on 1 March 2022 from https://www.w3.org/TR/vc-data-model/#data-first-approaches.
[33]Working Group, Verifiable Credentials Data Model v1.1., World Wide Web Consortium, Retrieved on 1 March 2022 from https://www.w3.org/TR/vc-data-model/#data-first-approaches.
[34]DH Web Desk, Fact-Check: Was Indians' vaccine data on Co-Win actually leaked? Here's what experts believe. Deccan Herald. Retrieved February 25, 2022, from https://www.deccanherald.com/national/fact-check-was-indians-vaccine-data-on-co-win-actually-leaked-heres-what-experts-believe-996239.html.
[35]Ethiraj, Govindraj. (2021, May 29). 'CoWin Vaccination Certificates Can Increase Mobility For Vaccinated Indians'. IndiaSpend. Retrieved February 25, 2022, from https://www.indiaspend.com/indiaspend-interviews/cowin-vaccination-certificates-can-increase-mobility-for-vaccinated-indians-751934.

Accessibility of the Vaccine Credentials.

Vaccine credentials are only available in digital formats. Many convenient channels have been established to ease the process of obtaining one's vaccine credential - the simplest of them being through WhatsApp. However, all these options require access to the Internet and the digital know-how to navigate at least one of the various applications (Co-WIN, Umang, Aarogyasetu, DigiLocker, WhatsApp, etc.)

Recommendations

- Digital Wallets: Data is stored locally in a special mobile application for the user or in the cloud so that only the user has access to their credentials. This is a decentralised storage approach.[36]
- The VC system should be designed to ensure that single-use verifiable credentials are operational. This will mitigate any harms associated with correlation and can ensure data is continually updated.[37]
- Ensure VCs can incorporate digital identities for machines since identification and authentication of users can take place through their devices.[38]

Single Source of Truth: Exclusionary Effects

As InDEA 2.0 adopts one of the informational principles, i.e., single source of truth as a core building block value proposition, it is essential to acknowledge the unintended consequence of exclusion at different stages of identification illustrated and discussed below.

Figure 2: Stages of identification

Enrolment: This is the stage at which governments enrol citizens to federated digital id, where they could exclude individuals who are not digital yet. Digital penetration has picked up pace in India. Still, it is yet to cover a considerable amount of mass, especially the low income and rural population (For instance, TRAI report states that internet subscription in rural India is only 36.24 per 100 population).[39] Therefore, using federated digital id as a legal id can exclude the population from some important services, as we see in the Aadhaar architecture for welfare targeting. In addition, the lack of clarity/scope of using other alternate documents, which is not a digital id as identity proof, complicates obtaining benefits.

Besides, figure 1 in this report sourced from the InDEA 2.0 document implies that almost every other registry id is linked to Aadhaar (others), making it a foundational id. In addition, the InDEA 2.0 also recommends government id providers strike an id alliance to bring coherence, interoperability, and reuse. While interlinking ids and

[36]Sedlmeir, Johannes et al. (2021). Digital Identities and Verifiable Credentials. Business & Information Systems Engineering 63(5): 603-613 (2021). Retrieved February 24, 2022, from https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1359/wi-1359.pdf.
[37]Working Group. (2021). Verifiable Credentials Data Model v1.1., World Wide Web Consortium, Retrieved on 1 March 2022 from https://www.w3.org/TR/vc-data-model/#data-first-approaches
[38]WFedrecheski G, Rabaey JM, Costa LCP, Calcina Ccori PC, Pereira WT, Zuffo MK (2020) Self-sovereign identity for IoT environments: a perspective. In: Global internet of things summit, IEEE
[39]Telecom Regulatory Authority of India. (2021, August 27). Telecom Regulatory Authority of India. Retrieved February 25, 2022, from https://www.trai.gov.in/sites/default/files/QPIR_27082021.pdf

having Aadhaar as a foundation could bring positive impact, making digital infrastructure as a backdrop would exclude communities from Federated Digital Identity Ecosystem due to the digital divide. For instance, while Aadhaar penetration stands at 95% userbase of m-Aadhaar & Aadhaar QR stands at 77%.[40]

Authentication: At this stage, various service providers authenticate individuals for respective services using federated digital id. The document states that stakeholders would use the federated digital id for authentication and eKYC purposes for service delivery. As authentication requires high standards of data integrity, we would like to flag that InDEA 2.0 doesn't have a mechanism for correction and updation of information in case of wrong entries. Besides, using InDEA 2.0 repository as a single source of truth can also cause a fall through the cracks due to a lack of cross-checking mechanism, increasing chances of false negatives and false positives in targeting benefits.[41]

Application: Finally, at this stage, the service providers deliver the service to the individuals or deny the same if they are not eligible for the service. While individuals can reach out to service providers for grievances related to the service, InDEA 2.0 lacks provisions on grievance redressal mechanism to solve problems related to federated digital id at the application stage (or at any other stage).

Recommendations

The InDEA 2.0 must ensure the process and procedures of authentication and eKYC using federated digital id is exclusion proofed using the below recommendations at different stages.

Enrolment

- Differentiation between federated digital id and legal id must be made clear.
- The framework should acknowledge that federated digital id created through the integration of repositories can be used for authentication while accepting alternative legal ids for the same purpose.

Authentication

- While this repository of data can act as a single source of truth, it is also essential to have a mechanism to cross-check and evaluate the integrity, cleanliness of the data, as state and non-state actors would use this for real-life interventions. For instance, mechanising periodic audits for both data collection methods and data could help in cross-check. Besides, comparing the data with an alternative database can also help determine gaps and mistakes in data points within the integrated repository.
- While various registries will have different data correction and update mechanisms, InDEA 2.0 must have a single overarching mechanism both analogously and digitally to correct and update information in federated registries. Establishing a single point of contact for correction and updates across registries will make it easier for individuals to navigate the system.

Application

- InDEA 2.0 must establish a dispute resolution mechanism for individuals and stakeholders to raise their issues with ecosystem and architecture. Besides, this mechanism must culminate into a feedback loop on the framework to evolve.

[40]State of Aadhaar: A People's Perspective. (2019, November 25). Good ID. Retrieved March 8, 2022, from https://www.good-id.org/en/articles/state-of-aadhaar-a-peoples-perspective/
[41]Falling through the Cracks: Case Studies in Exclusion from Social Protection. (n.d.). Dvara Research. Retrieved February 25, 2022, from https://www.dvara.com/research/social-protection-initiative/falling-through-the-cracks-case-studies-in-exclusion-from-social-protection/.

- In many cases, navigating the grievance management system for both individuals and entities is arduous, making it difficult to reach the designated portal. Therefore, we suggest incorporating an Interactive Voice Response (IVR) wing as part of the InDEA 2.0. This automated voice response system (through call) should navigate individuals (or entities) to reach the appropriate grievance portal, i.e., service providers' grievance redressal mechanism or dispute resolution wing of InDEA 2.0.

Harmonisation of Data sharing policies and integration frameworks

In addition to state-level data sharing policies discussed above, the InDEA 2.0 framework seeks every relevant domain(s) to develop a data-sharing policy that regulates and enables public data sharing. We want to note that this would cause confusion with the Draft India Data Accessibility and Use Policy 2022, which overarchingly covers various central government departments. In addition, we caution that the existence of various sectoral level data-sharing policies and integration frameworks could cause complexity in implementation. Some of the key existing data sharing policies are - **Draft Non-Personal Data (NPD) Governance Framework** [42](enables data sharing to unlock the economic benefits from NPD), **Geospatial datasets liberalisation**[43] [democratised the existing geospatial datasets (including government)], **Open Data initiative of the Government of India**[44] (provides access to Government-owned shareable data and its usage information in open/machine-readable format), **India Digital Ecosystem of Agriculture (IDEA) framework**[45] (links various publicly available data from various schemes to digitalised land records).

Recommendations

- The framework must bring harmonisation by weeding out the overlapping and conflicting scopes and bring them to congruence with other existing policies.

- A high-level coordination mechanism comprising various levels of government and relevant departments, ministries etc., must be instituted to enforce data sharing and integration in a coordinated way.

II. Competition Law

Insufficient analysis of open protocols in the Indian antitrust framework

The report recommends the use of 'open protocols', instead of a platform model to ensure healthy competition in the market. It suggests that platforms form a unified interoperable network through the use of open protocols; citing the success of existing networks like Unified Payment Interface (UPI) and Account Aggregators (AA). Further, the report cites the example of the world wide web, email and India's mobile phone network; which enable the co-existence of various players and interoperability due to underlying 'open protocols' like HTTP and GSM.

---

[42]*Report by the Committee of Experts on Non-Personal Data Governance Framework*. (2020, December 24). MeitY. Retrieved March 8, 2022, from https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf.

[43]*Guidelines for acquiring and producing Geospatial Data and Geospatial Data Services including Maps* (2021, February 15). Department Of Science & Technology. Retrieved March 8, 2022, from https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf.

[44]*Open Government Data (OGD) Platform India – An Overview*. (n.d.). MeitY. Retrieved March 8, 2022, from https://www.meity.gov.in/writereaddata/files/OGD_Overview%20v_2.pdf.

[45]*Consultation Paper on* IDEA. (2021, June 1). Department of Agriculture, Cooperation & Farmer Welfare Government of India 1st June 2021. Retrieved March 8, 2022, from https://agricoop.nic.in/sites/default/files/IDEA%20Concept%20Paper_mod31052021_2.pdf.

[46]Ministry of Electronics and Information Technology (MeitY). (2022, January). India Digital Ecosystem Architecture 2.0, Draft for Consultation (Ver 1.0 Jan 22), Retrieved February 24, 2022, from https://www.meity.gov.in/writereaddata/files/InDEA%202_0%20Report%20Draft%20V6%2024%20Jan%2022_Rev.pdf at Pg. 51.

Open protocols can present pro-competitive benefits due to their interoperability and decentralised nature. For instance, they can enable 'multi-homing', i.e., the practice of consumers making use of more than one platform providing a similar service, which is an indicator of healthy competition. However, Indian developments suggest open protocols do not necessarily insulate the ecosystem from anti-competitive conduct.

We will analyse a few examples used by the report to encourage the use of open protocols, i.e., UPI and GSM and highlight competition law concerns therein. In 2018, the Competition Commission of India (CCI) ordered an investigation into a UPI-based digital payments player in the country. Concerns primarily arose on mandatory use of the entity's own UPI based payment system for purchasing apps on the app store. The prima facie order of the CCI brought to light potential infirmities in the UPI framework. National Payments Corporation of India (NPCI) mandates interoperability among UPI apps, giving apps an option to enable integration either via the 'collect flow' or the 'intent flow' framework. In applications with the former framework, the customer enters the Virtual Payments Address (VPA) in UPI app and then gets a push notification for the collection of payment. On the other hand, in applications with the intent flow framework, the consumer selects the UPI payment option and is then shown a list of UPI apps that support intent flow and can then select her preferred app.[47]

The entity under scrutiny had integrated its own UPI app with the intent flow, whereas other apps could be used through the collect flow methodology.[48] The latter being a more tedious process, it had the potential to affect consumer preference in favour of the entity's own app, thereby potentially violating competition law and flouting the core integration objectives of open protocols and interoperability. Evidence also reveals that within the UPI framework, two entities have been able to corner a share of more than 82% in the Indian market.[49]Therefore, the belief that the use of an open protocol system will necessarily lead to healthy competition in the market is not well-founded.

In the Global System for Mobile Communications (GSM) market, competition law issues have been witnessed for years. On two occasions, the CCI has ordered investigations of abuse of dominant position pertaining to GSM technology in India through unfair licensing for patents.[50] [51] Even though an open protocol framework enables sharing of essential patents on fair terms, there still exists the potential of engaging in anti-competitive behaviour through unfair or discriminatory licensing by patent holders. Therefore, the impact of intellectual property rights in the open protocol framework is another aspect that needs to be studied before proposing the framework as the preferred tool to maintain healthy competition.

Recommendations

- A deeper analysis of the benefits of open protocol models from a competition lens needs to be done. Further, emphasis on issues arising out of the existence of intellectual property rights and grey areas in open protocol frameworks should be given.

- Existing open protocol frameworks in India, including GSM and UPI, should be carefully analysed for existing competition law risks. In the light of relevant findings, these risks should first be dealt with in existing systems before implementing similar models in furtherance of objectives of InDEA 2.0.

[47]Case No. 07 of 2020, Competition Commission Of India, Retrieved February 24, 2022, from https://www.cci.gov.in/sites/default/files/07-of-2020.pdf.
[48]Case No. 07 of 2020, Competition Commission Of India, Retrieved February 24, 2022, from https://www.cci.gov.in/sites/default/files/07-of-2020.pdf at Pg. 25 and 27.
[49]Chadha S., (2021, Dec 7), UPI emerges king of digital payments : PhonePe, Google Pay biggest players, Retrieved February 24, 2022, from https://timesofindia.indiatimes.com/business/india-business/upi-emerges-king-of-digital-payments-phonepe-google-pay-biggest-players/articleshow/88136978.cms.
[50]Case No. 04 of 2015, Competition Commission Of India, Retrieved February 24, 2022, from https://www.cci.gov.in/sites/default/files/042015_0.pdf.
[51]Case No. 76 of 2013, Competition Commission Of India, Retrieved February 24, 2022, from https://www.cci.gov.in/sites/default/files/762013_0.pdf

- The Ministry should involve more stakeholders, including competition lawyers, industry players and anti-trust scholars, while analysing these aspects. In addition to garnering various perspectives, this approach will also help highlight their concerns.

The Dialogue™

INFORM ENGAGE IDEATE

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

https://thedialogue.co