The Centre for Internet and Society's response to the:

Comments on InDEA 2.0

27th February 2022

By: Divyank Katira, Shweta Mohandas and Shruti Trikanand

The Centre for Internet and Society, India

Introduction

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with disabilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cyber-security. The academic research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies, and vice versa.

CIS thanks Meity for the opportunity to provide comments on the India Digital Ecosystem Architecture (InDEA) 2.0 Framework.

General comments

1. **Privacy framework:** The InDEA 2.0 is another policy report concerning the use of personal data that has come in the absence of a data protection law. While the report mentions principles such as privacy and security by design, data portability, data minimisation, purpose limitation these terms have not been defined in the report. This would mean that the extent and definition of these terms will be derived from the Data Protection Act. The data sharing principle states that policies stipulating data sharing will be in accordance with the applicable data protection legislation. Ideally the policy should come into force only after the Data Protection Bill becomes law to ensure that the policy is in compliance with the final text of the legislation, and to ensure that the data principals rights are not infringed.

2. **Membership:** We suggest that the steering committee and the working group have at least one member from civil society,especially from those working on privacy, data protection or human rights.

3. **Privacy by Design:** The report emphasises on the need to ensure privacy by design. The report enlists nine principles under privacy by design that requires adoption. While looking at privacy by design, there is a need to look at dark patterns in design which can alter the way information about privacy is seen and accessed by the individual. Example can be taken of GDPR, design choices could lead to inaccessible privacy policies while still the policies were in compliance with provisions of the legislations.[1] Additionally, privacy by design should not be limited to the privacy policy, and should be maintained at all stages of the data

[1] https://cis-india.org/internet-governance/blog/the-pdp-bill-2019-through-the-lens-of-privacy-by-design

processing. We suggest that the guidelines and principles of privacy and security by design should be formulated with the assistance of the design community, and accessibility researchers.

4. **Ecosystem Sandbox -** The report includes ecosystem sandbox as one of the technology enablers. The report also suggests the creation of a reference architecture for the sandbox. However there is a need to look at the current and proposed sandboxes, and to ensure that there is clarity and similarity between them. The Data Protection Bill also mentions under Clause 40 the creation of sandboxes, and sectoral sandboxes are already in place and functioning. Hence there is a need to look at how the sandboxes will work within different regulatory regimes. For example the Reserve Bank of India (RBI) has an established sandbox for the banking sector. For example, if a sandbox for the fintech sector was created, there would be a possibility of confusion over which regulation would they fall under;the architecture of the sandbox created under this report, the Data Protection Bill, or the RBI Guidelines.

5. **Mobile first -** While the report states that the delivery of all digital services would be through mobile by default, it fails to acknowledge the reality of mobile phone growth and use in India. While the report also states that there would be an offline option for "network-challenged geographies", it fails to recognise that there might be people living in cities who don't have access to a feature phone, let alone a smartphone. For example the GSMA mobile penetration report for 2018 notes a 23 percent gender gap in ownership of mobile phones and - only 63 percent women in India own mobile phones.[2] The framework emphasises on the need for mobile phones and an online only option it could act as an exclusionary barrier to a large number of the population both urban and rural, who will be limited due to the non availability of mobile phones.

6. **Federated Digital Identities -** Currently citizens possess many disparate functional IDs issued for different purposes (PAN Card, Voter ID, etc.), which are accepted as identification by various service providers. This system is already federated, in the sense that it allows individuals to choose the ID they wish to present while availing a service. What is being proposed is the increased digitisation of previously offline, paper-based ID registries, to enable their use for online authentication in the form of single sign-on. This lowers identification/KYC and authentication costs for various businesses and government departments, but comes with a compromise on user privacy.

   Our research on federated ID systems[3,4] in UK and Canada has shown that such systems are typically comprised of a centralised broker entity which mediates transactions between individuals, identity providers and relying parties.[5]

---

[2] https://cis-india.org/internet-governance/files/cis-comments-on-ndhb
[3] https://digitalid.design/decisions-guide/technological-design-choices.html#2.1
[4] https://digitalid.design/research-maps/uk.html
[5] https://digitalid.design/core-concepts-processes.html

While it is not clear whether the federated ID system proposed in the draft report would comprise of a central broker to mediate transactions, like those present in the federated ID systems in UK and Canada, or if the ID providers offering single sign-on will directly transact with the relying parties (similar to the sign-in services offered by Google and Facebook on various websites[6]), both approaches come with similar drawbacks. The broker or single sign-on provider learns a variety of metadata about individual users during the process of authentication. This includes the time, place and frequency of authentication, and the service that the individual is authenticating to. For instance, if one were to use a commercial single sign-on service to authenticate with a healthcare provider, they would learn which healthcare provider one goes to and how often the service is used, all of which is sensitive personal information.

The draft report proposes that this ID system be used as a core building block for several public and private services. This would result in a vast amount of metadata being generated as individuals go about their daily lives interacting with various digital services, which, in turn, can be used by ID providers to surveil their behaviours, habits and affiliations. It should be noted that the Supreme Court struck down the use of the Aadhaar ID system by some private institutions for similar reasons.

While the distribution of sensitive data among many ID providers is theoretically better than having a single large ID provider, the report also proposes digitisation of previously offline paper-based ID registries to participate in this federated system. This will lead to an overall increase in generation and sharing of private information and calls for careful consideration in design of the technology and regulation surrounding it.

Recommendations:

- Provide a detailed design of the proposed federated ID system, preferably with a working prototype implementation, so that researchers can better understand what is being proposed.
- Conduct and publish a cost-benefit analysis of the proposed digitisation of existing ID registries for their participation in a federated ID system.
- The proposed use of ID registries that have user-controlled uniqueness, which allows for individuals to transact privately and remain anonymous, should be the mandatory default and not simply a recommendation. (Recommendations to make user-controlled uniqueness more privacy-respecting are detailed below)
- Given the surveillance potential of ID systems, we should reduce reliance on individual consent as there is a vast informational asymmetry between the entities collecting data and individuals providing consent for use of their data.[7] If such a system must be built, there should be strong legal and

[6] https://developers.facebook.com/docs/facebook-login/
[7] https://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy

technological restrictions put in place on where it can and cannot be used before it is deployed. There should be public consultations on it's appropriate use.

7. **User Controlled Uniqueness -** We commend efforts to allow individuals to authenticate themselves anonymously and transact privately in cases where identification and uniqueness is not required. However, the draft report recommends that the unique identifiers chosen by the user can be common, easy to remember identifiers, such as mobile numbers and email addresses. The use of common identifiers encourages their re-use for multiple services, which is not conducive to privacy. For example, an individual may use the same phone number or email address to register for many different services. Such an identifier would allow service providers to track individuals across different services and can lead to re-identification of the individual in case any of the databases in question are breached.

   Recommendation: We recommend adopting a defensive approach when dealing with privacy, which accounts for things going wrong. As such, this identifier should be randomly generated and unique to every service that the individual interacts with to prevent malicious or intentional linking of disparate databases. The Web Authentication standard[8] is a good example of how to achieve this.

8. **Risk of re-centralisation-** A federated identity system allows users to choose between multiple identity providers that facilitate authentication across various platforms. This approach is praised for its privacy-enhancing ability, as it prevents the centralisation of data with one ID provider. The draft framework strongly encourages federated ID, with the goal of decentralising governance, and balancing the autonomy and needs of users/enterprises.[9] However, amongst the choices of different available digital IDs is Aadhaar, a strongly centralised digital ID that nearly every resident in India already possesses. In its recommendations, the framework suggests that users should always be allowed to use their Aadhaar ID as an identifier to achieve uniqueness when accessing registries (and where global state-controlled uniqueness is necessary, it is the *only* identifier allowed).[10] It also recommends that registries offer authentication/Single-Sign-On along with eKYC capabilities using the primary ID of that registry, to minimise a users' need to remember many IDs. In such a situation, both users and service providers are more likely to default to using Aadhaar to prove uniqueness. By introducing a popular digital identity provider into a decentralised system, it runs the risk of recentralisation,[11] in this case resulting in further centralisation of data with Aadhaar and the UIDAI.

---

[8] https://webauthn.guide/
[9] As explained in Annexure 2- Principles of Governance of Federated Architecture
[10] Section 4.3, InDEA 2.0 Framework
[11] For more, see https://digitalid.design/decisions-guide/technological-design-choices.html#2.4