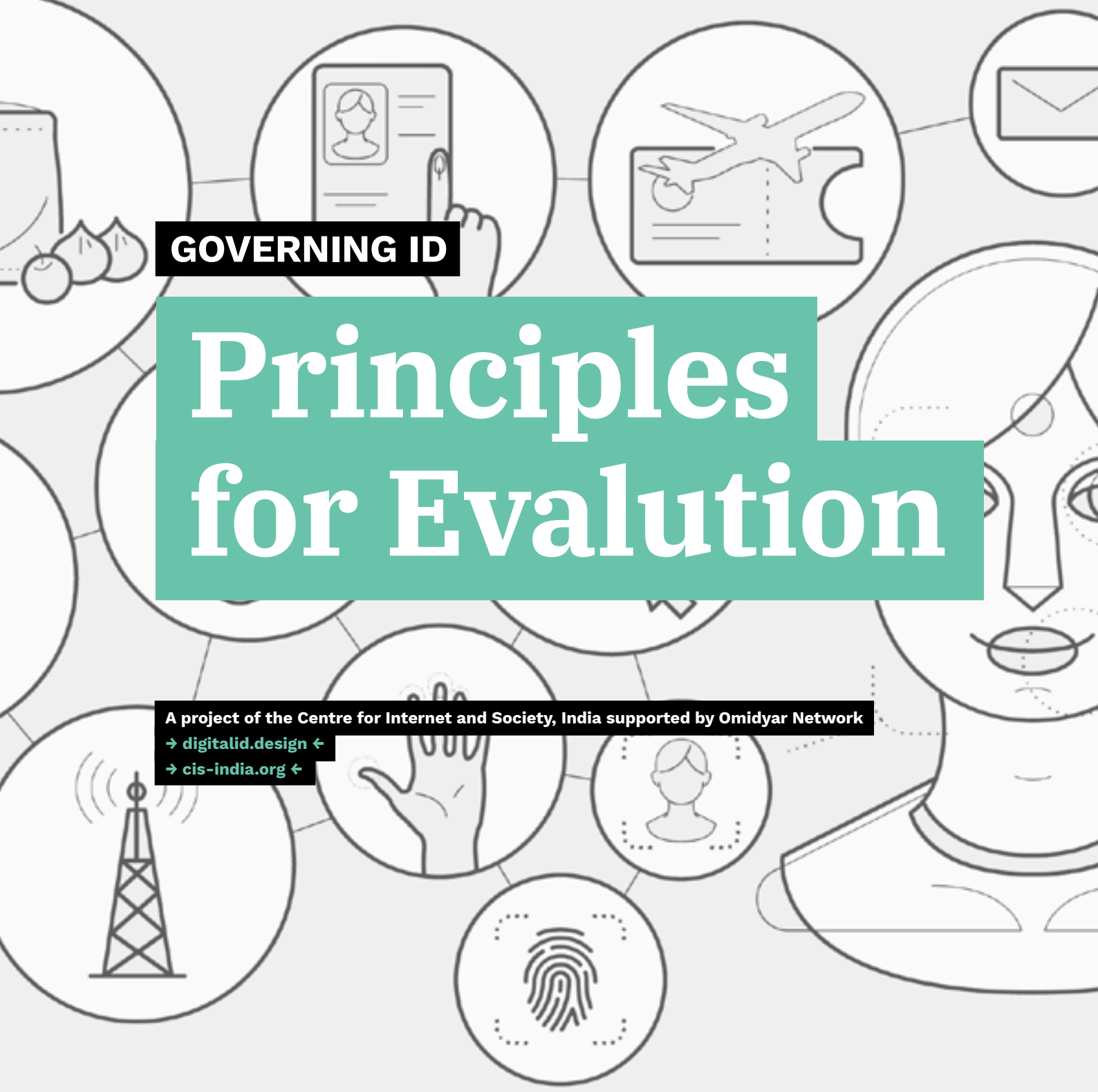

GOVERNING ID

Principles for Evalution

A project of the Centre for Internet and Society, India supported by Omidyar Network

→ digitalid.design ←

→ cis-india.org ←

RESEARCH & WRITING
Vrinda Bhandari, Shruti Trikanad, and Amber Sinha

REVIEW
Kaliya Young, Yesha Tshering Paul, and Sunil Abraham

DESIGN
Pooja Saxena

COVER ILLUSTRATION
Akash Sheshadri

Shared under
Creative Commons Attribution 4.0 International license

THE CENTRE FOR internet & society

TABLE OF CONTENTS

INTRODUCTION

As governments across the globe implement new and foundational digital identification systems (Digital ID), or modernize existing ID programs, there is an urgent need for more research and discussion about appropriate uses of Digital ID systems. This significant momentum for creating Digital ID has been accompanied with concerns about privacy, surveillance and exclusion harms of state-issued Digital IDs in several parts of the world, resulting in campaigns and litigations in countries, such as UK, India, Kenya, and Jamaica. Given the sweeping range of considerations required to evaluate Digital ID projects, it is necessary to formulate evaluation frameworks that can be used for this purpose.

This work began with the question of what the appropriate uses of Digital ID can be, but through the research process, it became clear that the question of use cannot be divorced from the fundamental attributes of Digital ID systems and their governance structures. This framework provides tests, which can be used to evaluate the governance of Digital ID across jurisdictions, as well as determine whether a particular use of Digital ID is legitimate. Through three kinds of checks — Rule of Law tests, Rights based tests, and Risks based tests — this scheme is a ready guide for evaluation of Digital ID.

RULE OF LAW TESTS

The rise of Digital ID, and the opportunities it presents, both for public and private actors, have in the past resulted in hasteful implementations and adoptions. This does not allow for sufficient deliberation to lead to governance mechanisms. Below are the most *basic tests* to ensure that a rule of law framework exists to govern the use of ID —

1.1 LEGISLATIVE MANDATE

Is the project backed by a validly enacted law? Does the law amount to excessive delegation?

Digital ID, by its nature, will entail greater collection and generation of personally identifiable information, and privacy risks, which arise from it. Any such restrictions to the fundamental right to privacy must be prescribed by law in the form of a publicly available legislative act. Other forms of regulation, such as executive ordinance, only meet this requirement in limited ways.

A validly enacted law has three components: (i) it should be passed by the Legislature, and not the Executive[1]; (ii) it should be accessible and foreseeable — this is to ensure the 'quality of law'; and (iii) it should be clear and precise — this is to limit the scope of discretion. Each of these three legal requirements is explained in some detail below —

(i) Legality

By its very nature, the collection, storage, and use of personally identifiable information through a Digital ID — especially if it has any mandatory requirements of identification, authentication, or authorisation — is likely to violate the right to privacy of the individual and affect their right to free speech, particularly as it leads to a chilling effect.[2] These concerns are exacerbated if the Digital ID is meant as a single online identity, that will more or less replace the use of existing functional identities, as was the case with several national identity programmes.

1 This is the legality prong of the proportionality tests used in most common law jurisdictions.

2 *US v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) noting that *"Awareness that the Government may be watching chills associational and expressive freedoms."*; Niva Elkin-Koren, Michal S. Gal, "The Chilling Effect of Governance-by-Data on Data Markets", 86 University of Chicago Law Review (2019): 403.

The rule of law requires that every act by the State or by its officers must, if it is to operate to the prejudice of any person, be supported by some legislative authority.[3] There should be 'a law', having statutory force and not a mere executive or departmental instruction.[4]

Thus, to pass constitutional muster, this infringement of a fundamental right or the invasion of life and personal liberty must be sanctioned by a law, having statutory force, enacted by the appropriate legislative body. This is the first prong of the proportionality test, as has been accepted key jurisdictions such as India,[5] UK,[6] Canada,[7] South Africa,[8] and by the European Court of Human Rights ('ECtHR') (as part of Article 8(2), European Charter of Human Rights' requirement of 'accordance with law').[9]

(ii) Quality of Law

Some courts have interpreted the legal standard of 'in accordance with law' as requiring 'quality of law', namely that the law is "accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law."[10] In this definition, foreseeability would require that the law be "sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any such measures."[11] While absolute certainty is not required as part of the 'foreseeability' requirement,[12] the rationale behind introducing these requirements is to prevent any arbitrary interference with fundamental rights by the State.[13]

3 *State of Madhya Pradesh v. Thakur Bharat Singh*, 2 SCR 454 (1967).

4 *Kharak Singh v. State of U.P.*, 1 SCR 332 (1964); *Bijoe Emmanuel v. State of Kerala*, 3 SCC 615 (1986), at paras 16, 19.

5 *K.S. Puttaswamy v. Union of India*, 10 SCC 1 (2017), paras 310, 325 (Chandrachud J.), 638 (Kaul J.) [*"Puttaswamy'"; K.S. Puttaswamy v Union of India (II)*, 1 SCC 1 (2019), at paras 147, 557 [*"Aadhaar Judgment"*].

6 *Provincial Picture Houses v. Wednesbury Corporation*, (1947) 1 KB 223.

7 *R v. Big M Drug Mart Ltd.*, (1985) 1 SCR 295.

8 *S v. Makwanyane*, (1995) 3 SA 391 (CC).

9 *Belvedere Alberghiera v. Italy*, 31524/96, (2000), paras 56-58.

10 *Uzun v. Germany*, 53 EHRR 852 (2010), para 60; *Perry v. UK*, 39 EHRR 3, (2004) para 45.

11 *Malone v. UK*, ECHR 10, (1984) para 67.

12 *Slivenko v. Latvia*, 48321/99 (2003).

13 *Malone v. UK*, ECHR 10, (1984).

(iii) Clarity and Precision of Law

The requirement of clarity and precision aims to make the law specific, so as to limit its scope. By regulating the exercise of discretion, it serves as an effective guarantee against abuse.[14]

In this context, the relevant factors to ensure legislative quality are the quality of the substantive content of the law governing Digital ID, its form and language, the manner in which it was implemented, and its 'effectiveness', i.e. its ability to produce the desired regulatory results.[15]

Further, it is a settled principle that a law is void if it is vague,[16] and a vague law is one which impermissibly or excessively delegates basic policy matters to the executive, or if the Legislature abdicate its duty of laying down adequate guidelines for the exercise of Executive power.[17] This can lead to arbitrary and discriminatory application of the law. In the context of a Digital ID law, the factors to consider are whether basic policy matters of collection, storage, use, and sharing of the personally-identifiable information have been delegated to a rule-making body that is part of the Executive.

1.2 LEGITIMATE AIM

Does the law have a 'legitimate aim'? Are all purposes flowing from a 'legitimate aim' identified in the valid law?

All the purposes for use of Digital ID thus, must correspond to a legitimate aim identified in the valid law.[18] The ECtHR has held that this legitimate aim should be "necessary in a democratic society," i.e., it must answer a "pressing social need."[19] It should not be based merely on political expediency.[20]

14 *Vukota-Bojić v. Switzerland*, ECHR 899, (2016) paras 73, 77; *Piechowicz v. Poland*, ECHR 689,(2012) para 212.

15 Victoria Aitken, "An Exposition Of Legislative Quality And Its Relevance For Effective Development," 2 *PROLAW Student Journal*, 1-43 (2013); Helen Xanthaki, *Drafting Legislation: Art and Technology of Rules for Regulation* (Hart Publishing, 2014); Vrinda Bhandari and Renuka Sane, "A Critique of the Aadhaar Legal Framework," 31(1) NLSIR 1 (2019) (forthcoming).

16 Timothy Endicott, *Vagueness in Law* (OUP, 2000).

17 *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972); *A.N. Parasuraman v. State of Tamil Nadu*, 4 SCC 683 (1989).

18 *Peruzzo & Martens v. Germany*, ECHR 743, (2013), para 34.

19 *S & Marper v. UK*, ECHR 1581, (2008), para 101.

20 For an analysis of ECtHR's jurisprudence on this point, see, Steven Greer, "The exceptions to Articles 8 to 11 of the European Convention on Human Rights", Human Rights File No. 15, *Council of Europe* (1997), *https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf*, at 14.

In the context of a Digital ID, some illustrations of a 'legitimate aim' may be "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[21] The burden of proof in such cases, must be on the State to demonstrate the legitimate aim of the proposed law.[22] The only overarching requirement of the 'legitimate aim' standard is that it should not operate in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.[23]

However, the legitimate aim is only one part of the proportionality test; any law governing Digital ID will still have to pass the proportionality test, which will be discussed below.

1.3 DEFINING ACTORS AND PURPOSES

Does the law clearly specify the actors and the purposes that would flow from the legitimate aim?

The legitimate aims for Digital ID must be identified in the law governing the project. Key vectors for determining the legitimacy of aims for such projects are the actors who use Digital ID, and the purposes for which Digital ID must be used.

(i) Actors

The law must clearly specify the actors, or a category of actors who may use the Digital ID. Actors include both the State and private actors; entities who may use the Digital ID, and agencies and databases to whom it may be connected in any way.

Privacy serves as a restraint on the power of the government and private entities.[24] Consequently, the Digital ID law would also have to clarify whether — keeping in mind the legitimate aim of the Digital ID and whether it was mandating the use of the ID to access any service — it would apply *equally* to State and private actors.

21 Article 8(2), European Convention of Human Rights, 1950; *Puttaswamy*, supra, paras 311-312.

22 *Mozer v. the Republic of Moldova and Russia*, No. 11138/2010, (Grand Chamber) (2016), para 194.

23 Principle 2, Necessity and Proportionality Principles, *International Principles on the Application of Human Rights to Communication Surveillance* (May, 2014) available at *https://necessaryandproportionate.org/principles#principle2*.

24 Daniel Solove, "10 Reasons Why Privacy Matters", *TeachPrivacy (blog)*, January 20 2014, *https://teachprivacy.com/10-reasons-privacy-matters/*.

There has been limited examination of Digital ID by the courts, keeping in mind these principles. For instance, in India, in *K.S. Puttaswamy v Union of India (II)*[25] ("Aadhaar Judgment") the court broadly struck down the use of the Digital ID programme by the private sector as being unconstitutional and disproportionate, enabling 'commercial exploitation' of biometric and demographic information by private parties, and due to concerns of possible profiling.[26][27] It is worth noting that more than the focus of private and public actors, how digital identity is used is important. While we have had limited experience with digital identification systems, private use of other identification programmes has also been regulated. In the US, states such as Alaska, Kansas, Maine, New Mexico and Rhode Island either restrict the solicitation of Social Security Numbers or prohibit denying goods and services to an individual who declines to give their Social Security Number by private parties.[28]

In light of the unresolved questions around private sector involvement in Digital ID, we believe that any law governing Digital ID should make clear (i) if and how private entities can use the Digital ID infrastructure created by the State? (ii) if so, can they mandate the use of a Digital ID to get access to private services such as banking and telecom? (iii) is the private sector's use of the

25 1 SCC 1 (2019).

26 Aadhaar Judgment, supra, para (447)(4)(h). For a further analysis on the Court's reasons for striking down Section 57 of the Aadhaar Act, see Vrinda Bhandari and Rahul Narayan, "In striking down Section 57, SC has curtailed the function creep and financial future of Aadhaar," *The Wire*, Sept. 28, 2018, *https://thewire.in/law/in-striking-down-section-57-sc-has-curtailed-the-function-creep-and-financial-future-of-aadhaar*.

27 Through an amendment and ordinance, the government has now sought to (re-)introduce voluntary private sector involvement in the Aadhaar and Other Laws (Amendment) Bill, 2019, with diverging views on whether this is legal and/or appropriate. For arguments on why the Amendment is contrary to the Judgment of the Supreme Court see Raghu, "Six Reasons Why the Aadhaar Amendment Ordinance Undermines Democracy," *The Wire*, Mar. 12, 2019, *https://thewire.in/government/aadhaar-amendments-ordinance-democracy*; Vrinda Bhandari, "Why Amend the Aadhaar Act Without First Passing a Data Protection Bill?", *The Wire*, Jan. 4, 2019, *https://thewire.in/law/aadhaar-act-amendment-data-protection*. For (opposing) arguments endorsing the government's amendment, see Rahul Matthan, "The Aadhaar Amendment and Private Sector Access", *LiveMint*, 08 Jan 2019, *https://www.livemint.com/Opinion/jmxPkXXGWeEfiAsCsA1xnO/Opinion--The-Aadhaar-amendment-and-private-sector-access.html*; Nehaa Chaudhari, "Supreme Court has banned private companies from using Aadhaar. What does it actually mean?", *Scroll.in*, October 4 2018, *https://scroll.in/article/896771/supreme-court-has-banned-private-companies-from-using-aadhaar-what-does-it-actually-mean*.

28 "State Laws Restricting Private Use of Social Security Numbers." Advocacy. Accessed August 21, 2019, *https://advocacy.consumerreports.org/press_release/state-laws-restricting-private-use-of-social-security-numbers/*.

Digital ID and its surrounding infrastructure fulfilling the legitimate aim of the law and the legitimate purpose of using the ID? and (iv) if private sector entities will be held to the same standards of accountability as the State.

(ii) Purposes

Similarly, the purposes or the category of purposes for which the Digital ID is used must always be backed by law and clearly and explicitly defined.[29] In a common law country, this can be done in the Statement of Objects and Reasons behind introducing the law, in the Notes and Clauses of the individual provisions of the law, or in the ministerial speech moving the law in legislature.

The data collected by the State for the fulfilment of the legitimate State aim must be used to fulfil only those legitimate purposes that flow from the said aim, the burden of proving which is upon the State.[30] The nature of data required to fulfill this legitimate aim must also be expressly specified. The Digital ID should not be used for any extraneous or unauthorised purposes,[31] such as surveillance.

A clearly defined purpose limitation[32] of the Digital ID will allows users to limit the collection and retention of personal data to what is 'strictly necessary' and exercise their rights to object to any processing that is not considered 'strictly necessary.'[33] It will also prevent expansion of the project by way of mission creep.

In the context of a Digital ID, for instance, if the aim of the ID is to authenticate users for the provision of services, the Legislature should consider whether it is necessary to collect the biometric information of an individual (or if demographic information would suffice), and if so, should this biometric information include fingerprints or DNA samples? The Digital ID law should also clarify whether the sensitive personal information collected for one purpose (e.g. for provision of benefits) can be used for an entirely *unrelated* purpose (e.g. SIM card authentication). Ideally, it should

29 Access Now, "National Digital Identity Programmes: What's Next?", March 2018, 22 *https://www.accessnow.org/cms/assets/uploads/2018/03/Digital-Identity-Paper-digital-version-Mar20.pdf*. ["AccessNow"]

30 Principles 3 and 5, Necessity and Proportionality Principles, *International Principles on the Application of Human Rights to Communication Surveillance* (May, 2014), *https://necessaryandproportionate.org/principles#principle3*.

31 *Puttaswamy, supra*, para 311.

32 *Puttaswamy, supra.*

33 AccessNow*, supra*, 23, 25.

not, and any change of purpose/new purpose should be notified to the data subject for fresh consent.[34] Finally, a well defined purpose will enable citizens to determine whether centralised storage or long term retention of their data is necessary to achieve the purpose of the national Digital ID law.[35]

1.4 REDRESSAL MECHANISM

Does the law provide for adequate redressal mechanisms against actors who use the Digital ID and govern its use?

Adequate redressal mechanisms would necessarily include the following three requirements —

(i) User Notification

Individuals must be notified or at least be able to access information on when their Digital ID is used in any way, e.g. during every authentication procedure. This will allow citizens to be informed of every instance of usage of their personal data, as is with the case of credit and debit cards.[36]

There should also be proactive notification when there is a breach of their data. A national ID system, by its very nature, will be collecting and storing large swathes of sensitive and personal demographic, and possibly biometric information of the country's residents/citizens. The possibility of data breach thus, cannot be ruled out, and is especially dangerous when permanent identifiers like biometrics are used (which is another reason why biometrics should ideally not be a part of the Digital ID system). Hence, the Digital ID law should put in place legal requirements for the affected agency/data controller to notify the affected residents, as soon as a data breach occurs, and explain to them the impact of this breach.[37] This also ties in with the principle of accountability.

34 For instance, Section 15 of the Indian Census Act, the records of the census are not admissible as evidence in any civil or criminal proceedings. See also the 'Purpose Specification' Principle and the 'Use Limitation' Principle in the OECD Privacy Framework, *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*, at 14.

35 *S & Marper, supra*, para 103.

36 Nikhil Pahwa, "Learning from Aadhaar: 10 rules from nations on how not to make a mess of their digital IDs," *Scroll.in*, *https://scroll.in/article/858767/learning-from-aadhaar-10-rules-for-nations-on-how-not-to-make-a-mess-of-their-national-ids* ["Nikhil Pahwa"].

37 Report of the Group of Experts on Privacy, Government of India Planning Commission (October 16, 2012), *http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf*, ["Justice AP Shah Report"] 22, 70; AccessNow, *supra, 29*.

(ii) Access and Correction

The rights to access and correction are derived from the citizens' right to know, including their right to receive information, which are a part of the right to freedom of speech and expression.[38]

Individuals must have the right to access personally identifiable information collected through the use of Digital ID, to be able to confirm the data being held by the data controller, and to be able to obtain a copy of the same.[39] In the context of Digital IDs, this will enable the citizens to know the different agencies that have access to, and are able to process their digital ID information, including their biometric information. They should also have the ability to seek corrections, amendments, or deletion of such information where it is inaccurate.[40]

(iii) Due Process

A Digital ID law should have a well-designed grievance redress framework that addresses concerns of accountability, transparency, and user-friendliness.[41]

Individuals must be entitled to a fair and public hearing within a reasonable time by an independent, competent, and impartial judicial authority that is established by law, in cases where provisions of law governing the Digital ID are violated. This should take the form of adequate civil and criminal grievance redress mechanisms, with separate procedures for appeal. Appropriate remedies for damage caused due to violations or errors must be accounted for, including in the form of monetary compensation where necessary.

Civil redress mechanisms will have to be set up to deal with issues of omission or deactivation of the Digital ID (due to provision of false information or non-use), errors in the enrolment and verification process, or when there is an authentication failure (to prevent exclusion). All these acts have serious civil consequences of excluding citizens from the benefits of

38 *Indian Soaps & Toiletries Makers Association v. Ozair Hussain*, 3 SCC 641, (2013), at paras 28 and 29; *Reliance Petrochemicals v. Indian Express*, 4 SCC 592, (1988) para 34.

39 Justice AP Shah Report, *supra*, 25.

40 See in the context of general data protection legislation, Sections 45 (right of access) and 46 (right of rectification) of the UK Data Protection Act, 1998.

41 For elements of a well-designed grievance redress framework, see Vrinda Bhandari and Renuka Sane, *Critique of the Aadhaar Legal Framework, supra*, 18-20.

the Digital ID system, and thus, any adverse act (such as deactivating the ID, rejecting the enrolment, or denying benefits due to authentication failure) should be preceded by following due process and giving the aggrieved citizen a proper hearing.[42] It is also important that both civil and criminal redressal proceedings can be initiated by both regulators responsible for governance of Digital ID, as well as individuals — or class of individuals — who may be impacted.[43]

1.5 ACCOUNTABILITY

Are there adequate systems for accountability of governing bodies, users of Digital ID and other actors?

The collection, storage, and use of sensitive and personal information occasions a duty of care for its protection.[44] The laws governing Digital ID must provide for systems of accountability for the bodies that implement and operate the Digital ID, regulators, public and private actors which use Digital ID in any way, and other enabling or supporting actors.

The principle of accountability is a well-recognised privacy principle.[45] However, it is important to understand that accountability does not replace existing law, nor does it redefine privacy. Instead, it merely seeks to improve *privacy governance* and ensure effective compliance with existing laws to achieve the law's privacy objectives.[46] Given the vast enterprise of data collection, storage, and use that is carried out by the government and possibly private actors, individuals often have

42 *Sahara India v. CIT*, 14 SCC 151, (2008) para 29.

43 The Indian Aadhaar experience is instructive to understand the issues with criminal redress. Despite designating various actions as specific criminal offences, section 47 of the Aadhaar Act permitted only the UIDAI to initiate criminal prosecution, thereby eliminating the involvement of the Aadhaar number holder entirely. The constitutionality of this provision was challenged before the Supreme Court, which held *"Insofar as Section 47 of the Act which provides for the cognizance of offence only on a complaint made by the Authority or any officer or person authorised by it is concerned, it needs a suitable amendment to include the provision for filing of such a complaint by an individual/victim as well whose right is violated."* Subsequently, the government added a proviso to Section 47 through the Aadhaar Amendment Act, 2019, allowing the Aadhaar number holder or individual to file a criminal complaint for the commission of certain specified offences.

44 Privacy by Design: Current Practises in Estonia, India, and Austria, World Bank Group, 2018, *https://id4d.worldbank.org/sites/id4d.worldbank.org/files/PrivacyByDesign_112918web.pdf*, ["ID4D WB"] 5.

45 OECD Principles, *supra*; Justice Shah Report, *supra*, 27.

46 Accountability: A Compendium for Stakeholders, The Centre for Information Policy Leadership, 2011, *http://informationaccountability.org/wp-content/uploads/Centre-Accountability-Compendium.pdf*, at 3.

little knowledge or control over their personal data. Accountability thus assumes an even greater role in this context.

Accountability can be both *ex-ante* and *ex-post*,[47] and achieved through a variety of ways — better enforcement of laws, an effective regulatory framework, a proper delineation of responsibility amongst the various actors in the Digital ID system, transparency, user breach notification, and efficient grievance redress procedures.

In a Digital ID system, it can also take the form of requiring the Digital ID agency to maintain an access log (tracking who accessed the data, when, where, and for what purpose) that is associated with the identity for the user to consult at any time.[48] This will help prevent any misuse. If such logs are maintained, unauthorized access must be especially guarded against, as the logs, together with the metadata they generate, enable major inferences to be made about an individual. To that end, there must be a process to periodically delete or anonymise older logs. A legislation governing Digital ID should ideally also separate the role of the administrator, who is in charge of the storage of personal data and regulator, who licenses other agencies to perform enrolment and authentication functions and is in charge of grievance redress of the Digital ID program. There is an inherent conflict of interest if the same body performs both roles.[49] Thus, the Digital ID law should set up an *independent* and robust regulatory or monitoring framework, so that the administrator of the Digital ID can be held responsible for any breach in the database.

1.6 MISSION CREEP

Is there a legislative and judicial oversight mechanism to deal with cases of mission creep in the use of Digital ID?

Mission creep or function creep is the idea that a system or technology that has been developed for one purpose, or with one set of capabilities, ends up getting used for other purposes it was not originally intended for. These subsequent uses may be advantageous, but more often than not, are pernicious, and include

47 For a detailed discussion on ex-ante and ex-post accountability, see Vrinda Bhandari and Renuka Sane, NLSIR, *supra*, 13.

48 AccessNow, *supra*, 25.

49 See the observations made by Chandachud J. in his dissent in *Aadhaar Judgment*, para 1539.5 (Chandrachud J). See also NLSIR, *supra*.

profiling and surveillance.[50] Mission creep or function creep thus, ends up conflicting with the right to privacy.

Mission creep takes place on the back of data collected/generated through the use of a Digital ID. It is particularly problematic when the Digital ID captures biometric information, stores it centrally, and then uses it across different services (e.g. identification for a drivers' license to authentication for receipt of benefits), since the mission creep raises heightened concerns of surveillance.[51]

As time progresses, Digital ID systems have a greater probability of suffering from mission creep. To prevent mission creep, the governing Act must explicitly specify the proposed uses of the Digital ID and the particular data being collected. Further, it is important to explain to the individuals the nature of their personal information being collected, the purpose it will be used for, and the agency using it. This is also in line with the traditional notice and consent framework and the idea of informational self-determination. Thereafter, the executive authority must not be able to allow for attempts to use the Digital ID for newer purposes unless there is a proper legislative process for deliberating the additional uses, or a judicial examination of these uses against the legitimate aims, or a fresh consent sought from the citizens.

Some of the recognised mechanisms to limit mission creep are[52] —

> *"(i) limiting the amount of data that is collected for any stated purpose; (ii) enabling regulation to limit technological access to the system; (iii) concerted debates with all stakeholders and public participation; (iv) dispersion of multiple enablers for a system; and (v) enabling choices for user participation."*

The above strategies if specifically included in the law governing Digital ID, can help ensure that sensitive and personal information collected for one purpose does not end up getting used for another, unintended purpose. This will aid in constraining government power.

---

50 T.H.A. Wisman, "Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things", *European Journal of Law and Technology*, Vol. 4, No. 2 (2013), *http://ejlt.org/article/view/192/379#_ftnref11*; M. Granger Morgan and Elaine Newton, "Protecting Public Anonymity", *21 Issues in Science and Technology* (2004).

51 Nancy YueLiu, *Bio-Privacy: Privacy Regulation and the Challenge of Biometrics* (Routledge, 2012), 72-73 ["Liu"].

52 *Vinod Kumar v. Ashok Kumar Gandhi*, 1 SCC 1, (2019) para 1357.

RIGHTS BASED TESTS

The most clear and outright critiques of Digital ID systems have come in light of their violations of the right to privacy. Across jurisdictions, critics have discussed different forms of violations of privacy, including mandatory collection of sensitive personal data such as biometrics, lack of robust access-control mechanisms, inadequate protection of private sector collection of data, and increased behavioral profiling through use of one identifier for all services. Alongside, there have also been serious questions raised about exclusion concerns where absence of an ID or failures in its functioning can lead to denial of basic entitlements and benefits. Key rights-based principles are highlighted below —

2.1 NECESSARY AND PROPORTIONATE

Are the privacy violations arising from the use of Digital ID necessary and proportionate to achieve the legitimate aim?

The use of Digital ID may pose inherent risks to the right to privacy by leading to generation of more data, facilitating the connection of varied sets of behavioral data to unique identities, enabling greater surveillance, and involving new sets of actors. It is now well settled that the *mere* storage and retention of personal data for unspecified purpose or without regard for informed consent is a violation of the right to privacy.[53] The subsequent use or abuse of this stored information has no bearing on this finding.[54]

Given that privacy is not an absolute right, it is important to determine whether restrictions on this right are just, fair, and reasonable; and whether, on this basis, the Digital ID can be sustained.[55] Privacy violations arising from the use of Digital ID must satisfy the requirement of proportionality.

Under ECtHR law, an interference with the right to privacy is sustained if it is 'necessary in a democratic society', which, *inter alia*, requires it to be *proportionate* to the legitimate aim pursued, and the reasons adduced by the national

53 *Leander v. Sweden*, ECHR 4, (1987) para 48; *MK v. France*, ECHR 341 (2013); S & Marper v. UK, ECHR 1581, (2008), para 67.

54 *Amann v. Switzerland,* ECHR 88 (2000), para 69.

55 *Puttaswamy, supra*, paras 311, 328 (Chandrachud J.), 640 (Kaul J.)

authorities to justify it must be 'relevant and sufficient.'[56] Differing standards of burden of proof and margin of appreciation have been applied in proportionality inquiries under Article 8, ranging from a 'priority to rights' to 'balance' between the rights and exceptions.[57]

In *MK v. France*, the ECtHR held that the collection and retention of fingerprints of persons who had been accused, but not convicted of offences, on the grounds that it would 'rule out' their involvement in case someone tried to steal their identity 'would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant.'[58]

Under Indian law, violations of the right to privacy are justified if (i) they are pursuant to an existing law; (ii) there is a legitimate State aim; (iii) the proposed measure is proportional or bears a 'rational nexus' between the objects and means adopted to achieve the stated aim; and (iv) there are procedural guarantees against the abuse of State incursions into privacy.[59]

The content of the proportionality prong has been further elaborated as comprising (i) a 'legitimate goal' or proper purpose; (ii) 'suitability', namely that the law must be a suitable means of furthering the aforesaid legitimate goal; (iii) 'necessity', i.e. there must not be any less restrictive but equally effective alternative present; and (iv) 'balancing', since the measure must not have a disproportionate impact on the right holder.[60]

The Jamaican Supreme Court, relying on the Canadian proportionality decision in *R v. Oakes*[61] held that courts must take proper cognizance of 'any deleterious effect' of the proposed measure being pushed by the government to meet its objectives and that "greater the severity of the effect the more important the objective must be, furthermore the measure chosen needs to be shown to be the least harmful means of achieving the objective."[62]

For a Digital ID, the proportionality inquiry would take place at various parts of the project, starting from compulsory enrolment, if any; centralised retention

56 *S & Marper, supra*, para 101; MK v France, supra, para 33.

57 Steven Greer. *The exceptions to Articles 8 to 11 of the European Convention on Human Rights. Vol. 88. Council of Europe*, 1997, *https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf*, at 15.

58 *MK v. France, supra*, para 40.

59 *Puttaswamy, supra*, paras 310, 325, 638, 639.

60 *Aadhaar Judgment, supra*, paras 319, 494, 511.5 (Sikri J.)

61 1 SCR 103 (1968).

62 *Robinson, Julian v. The Attorney General of Jamaica* (2019) JMFC Full 04 ["Robinson"]

and storage of sensitive, personal information; and the use of the Digital ID without following purpose limitation principles or putting in place procedural safeguards. This analysis would also include determining whether an ID system is needed when its risks are grave; based on the needs and interests of the country. For instance, if a country intending to use an ID system to deliver subsidies and benefits, has a high occurrence of corruption in the middlemen delivering such services, and a large population that depends on government payments, then it may be able to justify a more invasive Digital ID. Here, societal interests, in terms of delivering essential benefits to a wide population, are high, and thus the proportionality test favours allowing an invasion of privacy of individuals. On the other hand, in a country where a smaller population depends on government benefits, and corruption amongst middlemen is scarce, then a Digital ID system with large privacy concerns may be harder to justify, and the legitimate aims of the State could instead be met by other means.

At each part, the law would have to satisfy the aforestated four requirements, including demonstrating that the Digital ID is the least restrictive method of achieving the government's stated goal. A proportionality inquiry will thus, take the form of examining whether the State could prove that *voluntary* enrolment would preclude it from achieving its stated goal of providing reliable identification.[63] It would also attach itself to questions about whether the State has failed to destroy the excess identity information collected; or whether it has enacted safeguards to ensure access control and purpose limitation.[64]

2.2 DATA MINIMISATION

Are there clear limitations on what data may be collected, how it may be processed and how long it is retained for, during the use of Digital ID?

As uses of Digital ID emerge, there will be a need to exercise the principles of data minimisation to ensure that only data which is necessary is collected; this data is processed only for legitimate purposes; and is stored for only as long as

63 *Robinson, supra*, para 247(B)(49).

64 Principle 5, Necessity and Proportionality Principles, *International Principles on the Application of Human Rights to Communication Surveillance* (May, 2014), *https://necessaryandproportionate.org/principles#principle5*.

necessary.[65] This will help mitigate the harm caused by a possible data breach or identity theft,[66] and reduce possible abuse of State power.[67]

Data minimisation has been defined as the 'practice of limiting the collection of personal information to that which is necessary to accomplish a specified purpose.'[68] Article 5 of the GDPR requires the processing of personal data to be 'adequate, relevant and limited to what is necessary'. We take a broad view of data minimisation as underpinning the principles of collection limitation, storage limitation/retention, use limitation and purpose specification.[69] After the purpose for which the sensitive and personal information has been collected is fulfilled, the data controller/administrator should delete this data permanently from its records.

Thus, data minimization will dictate the amount and type of information that needs to be collected and stored for a Digital ID. It also requires that the storage and retention of data be proportionate. The administrator of the Digital ID has to determine, for instance, whether the collection of biometric or health information is necessary for achieving the purpose of the Digital ID; or whether the automatic storage (instead of deletion) of all the metadata relating to an authentication transaction is proportionate. The ECtHR has held that the permanent retention of fingerprint and DNA of persons who are *suspects* in *any* crime, but have not yet been convicted is 'blanket and indiscriminate' to the object of crime prevention and detection.[70]

2.3 ACCESS CONTROL

Are there protections in place to limit access to the digital trail of personally identifiable information created through the use of Digital ID by both state and private actors?

65 See also *Robinson, supra*, para 247(B)(56).

66 AccessNow, *supra*, 31.

67 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (2018) *https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf*, 53.

68 White Paper of the Committee of Experts on a Data Protection Framework for India (2018), *https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf*, 104-105

69 See also Justice AP Shah Report, supra, 24; Debbie McElHill, "GDPR Data Retention Quick Guide", *Data Protection Network* *https://www.dpnetwork.org.uk/gdpr-data-retention-guide/*.

70 *S & Marper, supra*, paras 107, 114, 119.

Privacy risks to individuals from use of Digital ID arise both from generation of data, as well as access to the generated data. Therefore, adequate access control mechanisms would entail regulation of access to information generated as a result of the use of Digital ID, and limiting the actors who need, and are authorised, to use this information to achieve the specified purposes of the Digital IDs. Access control measures need to be introduced within the Digital ID law, or at the very least in the general data protection framework.

While determining access control, the law would have to consider the desired extent of private and governmental access to sensitive and personal information attached with the Digital ID, and whether different standards would apply to them. It would also have to take into consideration whether the personal data is being stored in a centralised or federated database, the time period of retention, and whether the Digital ID is being linked to multiple State and private databases. A Digital ID law should also clarify whether sharing of personal data and metadata (relating to the authentication transactions) amongst various agencies is permitted, and if so, should include specific rules (e.g. on consent to be taken of the Digital ID holder) to govern such practices.

One way of achieving access control is to prevent seeding, especially inorganic seeding. Seeding is the process by which the unique identification number associated with the Digital ID is seeded across various databases – the linking/merging of these different silos of data facilitates easier tracking, profiling, and surveillance.

Access control thus, becomes essential, and can only be properly enforced if there is an effective and efficient right to legal recourse, with strict civil and criminal penalties for acts such as accessing, using, publishing, or sharing information in the Digital ID with third parties/online.

2.4 EXCLUSIONS

Are there adequate mechanisms to ensure that the adoption of Digital ID does not lead to exclusion or restriction of access to entitlements or services?

The experience with Digital ID, particularly in the developing world, has revealed various causes for exclusion,[71] including due to poor internet connectivity,[72]

71 Anmol Somanchi *et al*, "Well Done ABBA?," 52(7) *EPW* (2017) *https://www.epw.in/journal/2017/7/web-exclusives/well-done-abba.html*.

72 Geeta Pillai, "Need internet to buy PDS rations? Go climb a tree," *The Times of India*, March 3, 2017, *https://timesofindia.indiatimes.com/india/need-internet-to-buy-pds-rations-go-climb-a-tree/articleshow/57437975.cms*.

fingerprints wearing out with age and manual labour,[73] disability,[74] and problems with the Point of Sale machines.[75] This proves that the exclusion is not simply a result of poor implementation, but rather, is a function of the design of the ID system, if for instance, it relies on the inherently probabilistic nature of biometrics.

If the intended use of ID could lead to denial or restriction of services or benefits to individuals, or categories of individuals, then there must be mechanisms to ensure that such individuals are not disadvantaged. It is important to note that this exclusion can occur even at the stage of identification, if the costs of obtaining a Digital ID make them inaccessible to some citizens; this can be in terms of the location of identification services, typically restricted to populated areas, or in terms of requiring complex documentation, etc.

Primarily, the law should not require *mandatory* authentication of the Digital ID to receive various benefits. As stated above, a low incidence of exclusion is inevitable, and will likely hit the marginalised sections of society the hardest. Thus, any Digital ID system should avoid prescribing mandatory use and should instead, provide alternative mechanisms for establishing their identity. In these cases, individuals must be able to use other forms of identification to seek access to services or benefits. Further, the Digital ID should facilitate offline and localised verification of the demographic or biometric identity.[76] Exclusion can also be avoided by ensuring data quality and accuracy, to ensure that there are no errors in the information collected and stored on the Digital ID.[77] Administrative procedure decisions involving location, language, and costs to obtain an ID could also be exclusionary factors that should be accounted for.

73 Staff, "In Telangana, worn out fingerprints key reason behind 36% Aadhaar verification failure in key govt. scheme:Report," *HuffPost*, April 7, 2017, *https://www.huffingtonpost.in/2017/04/07/in-telangana-worn-out-fingerprints-behind-a-whopping-36-authen_a_22029773/*.

74 Gaurav Bhatnagar, "Testimonies Reveal how Aadhaar has Brought Pain, Exclusion to Poor," *The Wire*, March 15, 2018, *https://thewire.in/government/aadhaar-right-to-food-pain-exclusion*.

75 Jahnavi Sen, "In Rural Jharkhand, Aadhaar Link to Welfare Schemes is Excluding the Most Needy" *The Wire*, September 26, 2018, *https://thewire.in/government/jharkhand-aadhaar-pds-pensions*.

76 Subhashis Banerjee, Subodh Sharma, "An Offline Alternative for Aadhaar-based Authentication," *Ideas for India*, September 24, 2018, *https://www.ideasforindia.in/topics/productivity-innovation/an-offline-alternative-for-aadhaar-based-biometric-authentication.html*; Reetika Khera, "Aadhaar Bill Debate" *Ideas for Change*, *https://www.ideasforindia.in/templates/i4ihome/images/author/Aadhaar-Bill-Debate-Reetika-Khera.pdf*.

77 Olivia White et al., *Digital Identification: a Key to Inclusive Growth* (McKinsey Global Institute 2019) 7, *https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx* ["McKinsey"]

The law should also provide for a grievance redress mechanism, following the principles of natural justice, where the aggrieved Digital ID holder (who has experienced authentication failure) is given a right to be heard. The administrator of the Digital ID must be held accountable for any failures in the Digital ID system, which can be achieved partly through judicial/independent oversight.

2.5 MANDATORY USE

In case enrolment and use of Digital ID are made mandatory, are there any valid legal grounds for doing so?

Whether enrolling into and specific uses of ID should be mandatory or not remains one of the most important questions in ID. An identity can be mandated in two forms. First, enrolment in a national ID program, as in Jamaica, where the National Identification and Registration Act ('NIRA') mandated the collection of biometric information from all Jamaican residents, at the pain of criminal sanction.[78] Second, mandating its use for the provision of certain services. For instance, in India, although enrolment in the identity program is not mandatory, every resident who pays taxes in India requires it. In effect, thus, it is mandatory for all tax-payers.

Even assuming a legitimate aim and limited purpose of requesting certain personal information (including biometric information), the government should always seek to provide an option amongst multiple forms of identities.[79] This option should extend to an opt out mechanism, with the individual retaining its access to the service (provided they produce an alternative form of ID), and with mandatory erasure of all collected personal information from the ID system.

In the NIRA Case ('*Robinson*'), the Jamaican Supreme Court held that the compulsion and deprivation of choice inherent in the mandatory collection of biometric information engaged the liberty interest of individuals and amounted to bodily interference. In the absence of any 'strong justification' for the absence of an opt-out provision, the mandatory collection provision (Section 20) was deemed not justifiable in a free and democratic society and thus, declared unconstitutional. The risk of misuse/abuse by the State and the deprivation of personal choice were held to outweigh 'any conceivable [public] benefit.'[80]

78 *Robinson, supra*, 205

79 AccessNow, *supra*, 23-24.

80 *Robinson, supra*, para 247(B)(19), (48), (52), 349.

Various benefits and services provided by the States are not State *largesse* or 'gifts' to citizens of a country. However, making access to these benefits contingent on the use and authorisation of only one form of Digital ID violates these citizens rights to choose how to identify themselves to the government in a reasonable and non-intrusive fashion.

Thus, keeping in view the importance of choice, consent, dignity, and informational self determination, enrolment in a Digital ID should not be made mandatory. This is especially true in the case of children. An identity that is made mandatory should be subject to strict legal tests, such as the need to obtain information that is strictly necessary to provide a service to an individual; whether there is a less restrictive method of obtaining personal information that will enable the State to provide the same service; what is the nature of the service for which the *use* of the Digital ID is being made mandatory; prevention of harm to others, and eligibility to undertake specialised tasks.

It is important to note the distinction between foundational and functional identity systems here. A foundational identity system is a core Identity System created to manage identity information for the general public, and to provide identity proof for a wide variety of public and private services. On the other hand, a functional identity system is designed to meet the needs of an individual sector, and is not designed for, though, in some cases, may be used for other purposes or in other sectors. Within specific sectors, it is much more acceptable to mandate the use of functional identity systems which pertain to them.

RISK BASED TESTS

The debate and discussion around Digital ID has centered primarily on the perceived or existing risks related to privacy, welfare, equality and inclusion. As a range of use cases of Digital ID emerge, laws and institutions governing Digital ID must be vigilant about the risks and harms emerging from them. This needs to be done with some urgency regarding the existing use cases of Digital ID, as well. A rights based approach is, by itself, not sufficient to address these challenges, and there is a need for greater paternalistic regulatory measures that strictly govern the nature of uses of Digital ID. Below we attempt to articulate some draft principles. These principles do not exist in most jurisdiction dealing with Digital ID, though there is now an increasing focus on harms assessment in prominent frameworks such as the GDPR.

3.1 RISK ASSESSMENT

Are decisions regarding the legitimacy of uses, benefits of using Digital ID, and their impact on individual rights informed by risk assessment?

Borrowing from principles of law that seek to protect consumers, laws governing Digital ID need to take into account tangible harms to individuals, have clear provisions on prevention and appropriate recovery for those harms, if they occur.

Digital IDs combine technology, big data processing abilities, with vast quantities of biographical data, that carry risks of profiling, surveillance, and chilling effects.[81] Other risks associated with Digital IDs include human execution errors, unauthorized use, exclusion of individuals, and surveillance.[82]

A risk-based approach to privacy requires that the digital ID system not be exclusively examined against constitutional rights guaranteed to individuals, but also against actual/potential tangible harms they may suffer. A risk-based approach to privacy does not act as a 'substitute for legal compliance'; instead, it helps the government/administrator identify the risks, prioritise them in an order of severity and probability; and act accordingly.[83] A risk-based approach thus allows the administrator to take the full benefit of the Digital ID, while being cognizant of, and protecting, the rights of the citizens.

81 *Robinson, supra*, para 237.

82 McKinsey, *supra*.

83 Jedidiah Bracy, "Demystifying the Risk Based Approach" *The Privacy Adviser*, April 30, 2014 *https://iapp.org/news/a/demystifying-the-risk-based-approach/*

Risk assessment requires identifying a 'privacy risk', i.e. a feared event, and the 'risk sources', i.e. the manner in which such a feared event can be reached and avoided.[84] In Digital IDs, these risks can be classified into various forms, such as —

(i) Privacy Harms

The invasion of the right to privacy through the unauthorised transfer of personal data or through mission creep; for instance, a foreseeable risk of linking a digital ID with individuals' financial data, is that of the data being used to inform credit scoring without their consent or knowledge. The risk sources associated with this will depend on the amount of financial data accessible through the Digital ID; the role of private (finance) companies; the security and infrastructure of the system, etc.

(ii) Exclusion Harms

The denial of benefits that are linked to authentication of the Digital ID; for instance, denial of access to (essential) services due to reliance on imperfect biometric authentication, or the use of online authentication where the availability of internet is poor.

(iii) Discriminatory Harms

The misuse of the date collected, generated, and stored to help profile certain individuals and target them for their political views. Discriminatory harms can also be connected to exclusion harms in cases of identification via fingerprints or other electronic means, since these are disproportionately harder for those belonging to the marginalised class.

Risk assessment is aided by the enactment of a data protection law *before* the national Digital ID law, since the former lays down the governing standards for data collection, retention, storage, use, and sharing policies, and also sets up a proper civil and criminal enforcement framework.

3.2 DIFFERENTIATED APPROACHES TO RISKS

Do the laws and regulations envisage a differentiated approach to governing uses of Digital ID, based on the risks it entails?

Implicit in a risks based assessment is governance that is specific to the nature of

84 CNIL, Methodology for Risk Management (2012) 7, *https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf*, ["CNIL"].

harm it is attempting to address. Drawing from Fred Cate's model of harms in data protection,[85] a differentiated approach may involve categorising uses as:

(i) *Per Se* Harmful

Where a use is always harmful, such as when the use of ID to collect and use alternative data proven to be predatory for credit scoring and lending or the use of personal information to commit fraud, the regulator could prohibit the use outright.

(ii) *Per Se* Not Harmful

The regulator may consider not regulating uses that present no reasonable likelihood of harm, such as where Digital ID is used simply as one of many forms of ID for identification purposes (such as passports and driving licenses).

(iii) Sensitive Uses

Where use of personal data is neither "per se harmful" nor "per se not harmful," the regulator may condition the use on several factors, such as aligning with a rights based approach and requiring the consent of the user. For instance, the use of Digital ID for identification via authorisation or authentication can lead to exclusion, and hence, the government should always provide for offline or alternative verification mechanisms so that no user is denied the benefits that are linked to the identification.

3.3 PROPORTIONALITY

Does the law on Digital ID envisage governance, which is proportional to the likelihood and severity of the possible risks of its use?

Regulation of Digital ID needs to be sensitive to the actual harms caused by its uses, and be informed by the severity and likelihood of the harm. The risk level is estimated in terms of severity and likelihood. Severity represents the magnitude of a risk. It essentially depends on the consequences of the potential impacts. Likelihood represents the probability of a risk to occur. It depends on the level of vulnerabilities of the supporting assets facing the level of capabilities of the risk sources to exploit them.[86]

85 Fred Cate, "The Failure of Fair Information Practice Principles" in Winn, Jane K., ed. *Consumer Protection in the Age of the 'Information Economy'*. London: Routledge, 2016.

86 CNIL, *supra*, at 8.

Risk assessment requires that the harms be clearly identified and graded on a scale of severity. After this, the risk factors for each of these harns should be delineated and graded based on the likelihood of occurrence. These diverse risks in the Digital ID system then have to be addressed in the law commensurately, using proportionate measures. For instance, a design involving the centralised storage of biometric data with robust security safeguards may have a remote likelihood of security risk, but have a very high severity in cases of breach. Biometrics, being permanent and unchangeable, pose a great risk of identity theft if they are stolen. Therefore, it is imperative for the government to seriously consider whether, as part of 'privacy by design', the Digital ID needs to be designed this way. A proportionality analysis at this stage would suggest using less restrictive measures – i.e. measures that reduce the likelihood of harm – to prevent ID theft, if the government does decide to go ahead with centralised databases (thus, keeping the severity of harm constant).

The risk of identity theft can be mitigated by not collecting permanent and irreversible biometric information, which once compromised, cannot be changed (unlike a credit card password). Even if biometric data were to be collected, it would be preferable if on-device authentication is conducted by using the biometric data as a 'password', instead of employing centralised cloud storage and authentication.[87] It would also be more secure— from a cyber security perspective[88] — to separate the agencies overseeing the collection/identification task with the authentication task. The law should also set up a strong grievance redress and enforcement mechanism. Finally, prompt action should be taken by the government in the face of a security risk.

While risks associated with a digital ID system might depend on the design and architecture of the system, the threats a system is susceptible to can be analysed based on its use. Threats can be indicated by the number of entities/actors attempting to breach the system, which would in turn depend on the incentives available to them.[89] The wider the scope of services associated with the digital ID, the greater the threats it faces, thus increasing the overall risk of the system. For instance, where the digital ID system is connected to financial data of individuals, incentives for breach range from theft to collecting data for credit reporting companies; where the digital ID is connected to individuals' mobile numbers, it becomes possible to trace their online activities, thus subjecting the system to political motives. A system that contains many vulnerabilities but

87 AccessNow, *supra*, at 31.

88 AccessNow, *supra*, at 27.

89 Dave Birch et al., "Digital Identity: Issue Analysis", June 8, 2016, *https://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf*.

has limited threats, because of the narrow scope of its service, would present as overall low risk.

In this way, the possible uses of a system form a large part of the risk assessment of the entire system, and must be proportionally factored into the regulatory structure. This could also take the form of requiring different identifiers or having different security measures based on a particular use of the system, where the system has multiple uses, with the intention of reducing the overall risk in the most cost and operational efficient manner.

Another example of a proportionality analysis using the risk assessment model deals with exclusion. While conducting a risk assessment, the authorities will have to take into account the nature of personal information being collected. It is well-recognised that while dealing with biometrics, 'human recognition systems are inherently probabilistic, and hence inherently fallible. The chance of error can be made small but not eliminated,'[90] making exclusion errors for some individuals an *inevitable* reality. These harms have to be clearly recognised in the law, which should incorporate preventive and remedial measures in the law itself. In the present case, for instance, the risk of exclusion can be reduced by making use of the Digital ID voluntary.

Some of the risks[91] inherent in a Digital ID system and possible governance solutions are listed here —

(i) Inaccurate Data Collection

This can lead to exclusion while accessing benefits. It is important for the law to provide the right to access and correction, so that any incorrect data can be quickly rectified.

(ii) Authentication Errors

Problems with processing of ID credentials can result in false positives or false negatives during authentication. The law should connect the identity of the individual to a unique number, and not limit it to a biometric identifier.[92] It may also help to improve data quality, the quality of the device capturing biometrics, and (ironically) collect more data, since a more expansive

90 National Research Council in Washington DC Report, "Biometric Recognition: Challenges and Opportunities, 2010, *https://dataprivacylab.org/TIP/2011sept/Biometric.pdf*, 1.

91 ID4D WB, *supra*, 1; Mckinsey, *supra*, vi.

92 Robinson, *supra*, para 247(B)(48), (53). See also Liu, *supra*, 36-54.

database may reduce the risk of false positives.[93] Allowing alternate means of authentication where possible would help mitigate the harms of failure.

(iii) Mission Creep

The use of collected data for an extraneous purpose, without the user's consent, results in mission creep or an unauthorised use of data. Given the possible risks of this use, the Digital ID law should clearly incorporate the principle of purpose limitation, and require that each new use of data require a fresh consent. The law should also stipulate a wide range of civil and criminal penalties for various acts, and should have a strong grievance redress and enforcement mechanism. Besides having criminal or civil penalties, there must also be a strong oversight mechanism/body to identify when such harms are occurring, and means to address the harm itself, including mandatory deletion of data etc.

(iv) Indiscriminate Data Sharing

The potential of indiscriminate sharing or transfer of data between the regulator of the Digital ID, various State and private agencies, and third parties, poses significant privacy risks. Again, the law should criminalise such actions, and have a strong enforcement system. For instance, allowing citizens to access information about where their data is going, implementing a mechanism to always record flow of data, with time logs etc, are best practises to prevent unauthorised data sharing.

(v) Identity Theft

This remains a key risk of any identification scheme, if not done properly. Even though the Digital ID has very secure systems of collection and storage, even one instance of data theft, howsoever remote the possibility, can have potentially irreversible consequences (especially if biometrics are compromised). Hence, it is very important to prepare for such an eventuality – by implementing access control, limiting retention periods, criminalising such actions etc. Having a national data protection law and judicial oversight mechanisms already in place is also necessary to instil good data collection and storage practices and have a strong *working* enforcement system.

93 "Reducing False Positives without Increasing Regulatory Risks White Paper", Oracle, last accessed August 1, 2019 *https://www.oracle.com/technetwork/middleware/ows/documentation/ows-reducing-false-positives-wp-1864957.pdf* (webpage discontinued)

3.4 RESPONSE TO RISKS

In cases of demonstrable high risk from uses of Digital ID, are there mechanisms in place to prohibit or restrict the use?

Responding to risks that are inevitable in a Digital ID system are crucial to the functioning of the system. The World Bank recommends a two pronged approach to mitigating risks — first, conducting an 'ID Enabling Environment Assessment (IDEEA)' to study a country's legal and regulatory data privacy framework and highlight areas of improvement; and second, incentivising Privacy by Design features within the Digital ID law itself.[94]

For instance, the ID enabling environment can mitigate risks by making the Digital ID just one of the multiple choices and identities by which citizens can identify themselves. This is because a data breach or a security shortfall will not compromise the *only* ID that people have. For instance, if the national ID is the *only* accepted ID for operating a bank account, getting a SIM connection, and receiving benefits from the State; then any single security failure will compromise the entire security database.[95]

A Privacy by Design approach can be adopted by using derived/temporary identification numbers that mask the actual Digital ID number, which means that even in case of a data breach, the actual ID is not exposed.[96] For instance, Austria's national ID system has used 'tokenization' as a privacy by design principle.[97] The Indian government is also attempting to use Virtual IDs and tokens in place of the Aadhaar number.

Among other factors that must be considered while responding to a risk is that of the nature of the risk/harm. When a breach or failure of the ID system occurs in some manner, the effects can be either reversible or irreversible, notwithstanding the severity of the harm. For instance, if financial information of an ID holder has been accessed, while the harm is significant, it can be addressed by notifying the financial institutions, invalidating the ID credentials, etc. On the other hand, where personal information about an ID holder has been used to profile them, or to influence their choices like in the instance of the Cambridge Analytica data breach, the effects cannot easily be reversed, even by subsequently closing off the breach. Thus, even where the severity of the breach itself may not be very

94 ID4D WB, *supra*, 2.

95 Nikhil Pahwa, *supra*.

96 Nikhil Pahwa, *supra*.

97 ID4D WB, *supra*, 18.

significant, the irreversible nature of the harm warrants attention.

For the risks that continue to remain in Digital ID, due to the benefits that the system introduces to society, a mitigation strategy must be employed. This could involve a duty to notify ID holders of any breach to their data; establishing a body to prevent and investigate cyberthreats; having in place a (tested) business continuity plan to regain regular operations; investing in capacity building, etc. This risk mitigation strategy would also depend on the model and design of the digital ID system, and its reliance on private companies to provide IDs, authentication services, collect information etc.

If the risks from uses of Digital ID are demonstrably high, they need to be restricted until there are adequate mitigating factors that can be introduced. This may need a responsive Digital ID regulator, who has the mandate and resources to intervene responsively. In Estonia, for example, when a security flaw in around 750,000 national Digital ID cards came to light in 2017, making the ID cards susceptible to identity theft, the government took immediate preventive action and declared that the security certificates of the ID cards would be disabled.[98] They eventually laid out the lessons learnt from managing the risks.[99] ■

98 AccessNow, supra, 9; Aili Vahatla, "Estonia Cancels Security Certificates of 11,100 electronic ID cards", ERR News, June 1, 2018, *https://news.err.ee/836259/estonia-cancels-security-certificates-of-11-100-electronic-id-cards*.

99 "What we learned from the eID card security risk?," e-estonia, last accessed January 22, 2019, *https://e-estonia.com/card-security-risk/*.