THE CENTRE FOR internet & society

Towards a framework for evaluation of Digital ID

16.9
By 2030, provide legal identity for all, including birth registration

UN SUSTAINABLE DEVELOPMENT GOAL

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

What follows is an attempt to build draft principles against which Digital ID may be evaluated. We hope that these draft principles can evolve into a set of best practices that can be used by policymakers when they create and implement Digital ID systems, provide guidance to civil society examinations of Digital ID and highlight questions for further research on the subject. We have drawn from approaches used in documents such as the *necessary and proportionate principles*, the *OECD privacy guidelines* and scholarship on harms based approaches.

When we refer to the 'use' of ID below, we mean the use of digital ID to identify or authenticate ID holders, or make authorisations of any kind on their behalf.

Rule of Law Tests

The rise of Digital ID, and the opportunities they present, both for public and private actors, has often 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?

Digital ID, by its nature, will entail greater collection of personally identifiable information, as well as privacy risks. Any such restrictions to

fundamental rights 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.

1.2 DEFINING ACTORS AND PURPOSES

Does the law clearly specify the actors and the purposes?

The law must clearly specify the actors, or a category of actors who may use the Digital ID. Actors include entities who may use the Digital ID, as well as agencies and databases to whom the it may be connected in any way. Similarly, the purposes for which the Digital ID is used, while may not be expressly defined, must always be clearly backed by law.

1.3 LEGITIMATE AIM

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

All the purposes for use of Digital ID must correspond to a legitimate aim identified in the valid law. This legitimate aim must be "necessary in a democratic society," and not based merely on political expediency.

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: a) *User Notification*: individuals must be notified when their Digital ID is used in any way; b) *Access and Correction*: individuals must have access to personally identifiable information collected through the use of Digital ID, and the ability to seek corrections, amendments, or deletion of such information where it is inaccurate; c) *Due Process*: individuals must be entitled entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial judicial authority, established by law in cases where provisions of law governing the Digital ID are violated.

1.5 PURPOSES

If legitimate aims for Digital ID correspond to its specific purposes, does the project restrict itself to the uses which directly relate to such purposes?

Once the law or its supporting documents specify the legitimate aims of the Digital ID, all purposes must flow from this 'aim', and all uses of the Digital ID must have a rational nexus to these purposes.

1.6 MISSION CREEP

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

In cases where there is an attempt to use the Digital ID for newer purposes, the executive authority must not be able to allow for such uses in the absence of a legislative process for deliberating the additional uses, or their judicial examination against the legitimate aims.

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 PRIVACY VIOLATIONS

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, and involving a set of actors. Privacy violations arising from the use of Digital ID must satisfy the requirement of being necessary for achieving the legitimate aim. This means it must be the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon the privacy rights. Additionally, the privacy violations caused by the use of Digital ID must be proportionate to the legitimate aim being pursued.

2.2 ACCESS CONTROL

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

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 access to information generated as a result of the use of Digital ID would be limited to actors who need this information to achieve specified purposes.

2.3 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?

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 mechanism to ensure that such individuals are not disadvantaged. In these cases, individuals must be able to use other forms of identification to seek access to services or benefits.

2.4 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. As mandating ID limits the agency of individuals, it 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, prevention of harm to others, and eligibility to undertake specialised tasks.

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?

Drawing from consumer protection laws, laws governing Digital ID need to take into account tangible harms to individuals, have clear provisions on prevention, and for appropriate recovery for those harms, if they occur.

3.2 PROPORTIONALITY

Does the laws 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 harm. For instance, a design involving the centralised storage of biometric data

with robust security safeguards may have a remote likelihood of security risk, but has a very high severity in cases of breach.

3.3 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?

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.

3.4 DIFFERENTIATED APPROACHES TO RISKS

Do the laws and regulations envisage a differentiated approach to governing uses of Digital ID, based on the likelihood and severity of risk?

Drawing from Fred Cate's model of harms in data protection, a differentiated approach may involve categorising uses as (a) *Per Se Harmful*: where a use is always harmful (e.g., the use of ID to collect and use alternative data proven to be predatory for credit scoring and lending), the regulator could prohibit the use outright; (b) *Per Se Not Harmful*: the regulator may consider not regulating uses that present no reasonable likelihood of harm; and (c) *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. ■