Enhancing Digital Civic Space through OGP

Navigating the Risks and Rewards of Digital ID Systems

According to a 2022 United States Agency for International Development (USAID) report, the “roughly 1.1 billion people” lacking official identity are in many ways “invisible, discounted, and left behind.” Without a national identity, these individuals face barriers to accessing public services, exercising voting rights, and, in some cases, utilizing services offered by the private sector, like bank accounts and SIM cards. Indeed, the Sustainable Development Goals (SDGs) call on UN member states to provide legal identity for all, including free registration at birth, as one means to bridge socio-economic divides.

Governments are answering this call, in part, through digital ID systems, which electronically collect and store a set of credentials or attributes, including physical or behavioral attributes, that uniquely identify a person. A 2023 study by the Centre for Intellectual Property and Information Technology Law (CIPIT) at Strathmore University found that 22 of 27 countries assessed in Africa, the Balkans, Central Asia, Latin America and the Caribbean (LAC), and South and Southeast Asia had adopted digital ID systems, in many cases with biometric features.

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

Open
Government
Partnership

Open government thrives when people can freely access government information and services, share opinions and information among themselves and with their leaders, and act individually and collectively to influence decision-making and hold governments accountable—both online and offline. While the internet and digital tools can play an important role in empowering the public, more action is needed to ensure that these spaces enable robust civic action and participation. This series highlights the recommendations from the International Centre for Not-for-Profit Law's *Enhancing Digital Civic Space through the OGP Process*.

Risks and Rewards

The right to seek and share information is a fundamental element of free expression and a core component of the freedom of association and assembly. When identification systems make it harder to seek information or increase the threat of surveillance and harassment, they impede these fundamental freedoms.

- Digital-only systems may exclude those without access to the internet or mobile devices, or exacerbate other factors constraining participation. Individuals who cannot access other identification documents may also be locked out of digital ID services. And when digital IDs are legally required to register SIM cards, participate in deliberative policy-making, or access information from government portals, this establishes another barrier to free expression and access to information.
- Inadequate security measures can lead to data breaches or misuse of data by private actors and governments. Without due process to remedy and redress these issues, individuals may have compromised identities as well as suffering theft, extortion, fraud, and harassment. The prospect of digital ID-facilitated surveillance or misuse may also discourage members of the public from expressing their views, or sharing information, including about government initiatives.
- Without the ability to seek or share information or seek redress, individuals cannot participate fully in civic life or the economy, worsening poverty and exclusion.

These risks are more than hypothetical. The CIPIT study noted above drew on national and regional research conducted by an array of partners, with support from the Greater Internet Freedoms (GIF) project implemented by Internews and the GIF Consortium, to compare digital identity usage, threats, and impact across the countries noted above. Of the 27 countries assessed, 18 are either OGP members or affiliates, or currently eligible to join the Partnership.

The results are sobering.

- **Balkans:** The regional study of the Balkans found a “growing reliance on biometrics and digital identity (BDI) for online banking, e-government services, and border control,” even as the region has experienced a surge in data breaches, leaks, and cyber-attacks on critical infrastructure and public servers—suggesting that the shift to digital ID poses substantial risks to the privacy rights and personal information of ID holders.
- **Africa:** The report on biometrics and digital ID in Africa disclosed growing investments in biometric digital ID programs and collection of personal data, notwithstanding weak legal and institutional frameworks for data protection and civil registration. Key stakeholders have been excluded, moreover, from the development of these programs. The result: heightened apprehension among the public about the risks posed by these programs to privacy rights.
- **South and Southeast Asia:** The regional report on South and Southeast Asia reveals “opaque, ongoing collaboration between governments and third-party private entities, such as providers of BDI infrastructure or in-country private actors with access to BDI systems.” Governments have also applied “exclusionary practices observed in traditional ID methods” to digital ID systems, to the especial detriment of vulnerable communities.
- **Latin America and the Caribbean:** The report on digital ID systems in the LAC region concludes that “ambiguity latent in the ‘digital ID’ concept has enabled LAC countries to continuously expand the legal remit of their digital ID databases beyond identification to encompass any purposes marked as a state need.” This illustrates the significant risk that digital ID systems will be integrated into broader structures of state surveillance.

Inattention to open government and democratic principles in the implementation of digital ID systems increases the risks posed by these systems: data breaches and threats to privacy rights, exclusion of marginalized communities, and co-optation to advance state surveillance efforts.

However, as the GIF reports note, some of the countries assessed have adopted standalone, unified data protection legislation that, if effectively implemented, could help ensure the protection of personal information collected through digital ID systems.

- In the **Philippines**, legislation establishes safeguards to prevent the sharing of personal information, meant for identification purposes, with third parties and for other purposes.
- **Sri Lanka** has provided for the establishment of district-level Registration of Persons Tribunals, so that applicants may appeal decisions relating to the national identity card and database.
- **Brazil** adopted its new digital ID system through a legislative reform subject to ordinary deliberative processes, rather than through unilateral executive action.

There are good examples of positive practices respecting digital ID from beyond the GIF studies as well. The government of **Australia**, for instance, is working on draft legislation that would prevent law enforcement from accessing information from a digital ID system without a warrant.

But much more remains to be done to ensure that digital ID systems are adopted and implemented in a way that prioritizes public participation, inclusion, transparency, protection of privacy rights, and opportunities for redress where rights and requisite procedures are violated.

Recommended Open Government Commitments and Approaches

In implementing digital ID systems, governments should:

- **Conduct a robust human rights and privacy impact assessment** prior to designing or adopting a digital ID framework, that includes risk mitigation measures to ensure that the data of citizens and residents are protected. The assessment should be transparently shared and open to feedback from the public.
- **Refrain from collecting and integrating biometric data** as part of a digital ID system until the government can guarantee the data can be collected accurately and securely and the data can be stored without the risk of unauthorized access.
- **Implement digital ID as a voluntary government service** through which citizens and residents can enroll if they prefer to manage their government interactions digitally. Continue to allow individuals to prove their identity using conventional identification. Invest specific resources and effort in programs to promote access by marginalized populations to digital ID systems.
- **Develop and implement robust and proportionate legal frameworks**, through public processes of consultation with all relevant stakeholders, to govern use, operation, and access to digital ID systems and databases. Legal frameworks should consist of laws, policies, regulations, and codes of practice, and should establish independent oversight mechanisms, and include accessible grievance and redressal mechanisms to address violations of requirements and protected rights.
- **Refrain from establishing digital ID systems as a centralized repository** that government officials or private actors can easily access without limitations, particularly if the digital ID system includes biometric data. Access to the data should be strictly limited, and law enforcement access should be predicated on a warrant issued by an independent judicial authority.
- **Mandate public disclosure of procurement contracts and public-private partnerships** to develop and implement digital ID systems, as well as information about permitted uses and storage of, and access by public and private actors to, information collected through these systems.

- **Work with businesses and civil society** to develop and implement awareness campaigns, educational programs, and training initiatives, for the public and responsible government officials, to share information regarding digital security threats and best practices to promote cybersecurity, including with respect to the handling of personal information and digital IDs.

Members of the open government community can learn more about principles and positive practices for implementing digital ID systems, and other recommended reforms, by consulting ICNL's recent guide to *Enhancing Digital Civic Space Through the OGP Process*. By working together and keeping open government principles and values in mind, civil society and government reformers can help to mitigate risks posed by technologies like digital ID while ensuring they deliver on their promise.

Photo by Kenny Eliason via Unsplash