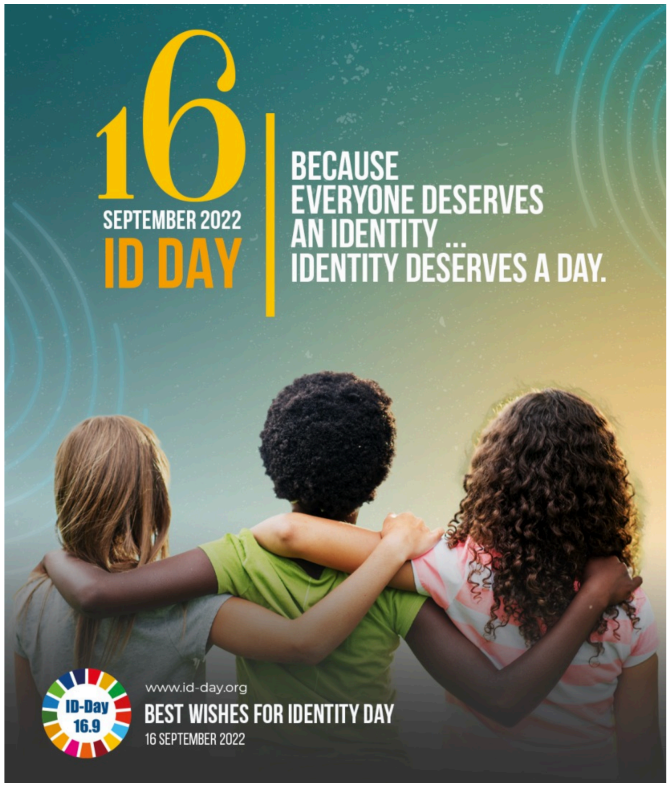
WORLD **PRIVACY** FORUM



Identity ecosystems are a central aspect of global digitalization; the principle of *Do No Harm* must be a policy priority and commitment

16 September 2022, International Identity Day

by Pam Dixon, Founder and Executive Director, World Privacy Forum

Identity is a data-rich resource that acts as a key to connect all levels of emerging digital ecosystems. All forms of ID carry some risk, but digital forms of ID, or "dematerialized ID," cuts across all sectors and links copious data about individuals, their behaviors, financial status, associates, and potentially even political and religious views. Over time, distinct patterns emerge from the linked data and create new kinds of risks for individuals and groups.

As the world becomes increasingly and intensely digitalized, we can expect challenges in the identity space to grow apace unless proactive attention is given to identifying and mitigating the current and future risks. While risks associated with biometrics use in digital identity ecosystems attract much attention now, there are in actuality many different kinds of risks in identity ecosystems. For example, exclusion is a profound risk. As has been documented by multiple NGOs, in Kenya some individuals are not granted the right to have an identity. Those who lack a formal identity find it difficult or impossible to purchase a home or engage in

activities that those who have an official form of proof of identity take for granted.[1] Intentional exclusion of people from identity ecosystems is a harm, and especially so when it results from political forms of exclusion based on, for example, religion or ethnicity.

Other circumstances present other kinds of harms. Recently, there was a large breach in China of up to an estimated 800 million records online which included high-resolution images of faces combined with license plate data and resident ID numbers.[2] This, too is a harm, because it increases the risk of serious cases of fraudulent uses of identity and other abuses of the identity information.

From time to time, some countries propose collecting DNA for their national identity systems.[3] There are some policies which should be designated as agreed-upon areas where identity systems should never go, and DNA collection for a national ID system is among them. Use of DNA creates the possibility for profound harm, particularly in regards to the risk that the national identity ecosystem becomes a magnet for law enforcement investigations without due process. Additionally, the loss of trust this kind of policy creates can be irreparable.

India provides one of the most important identity ecosystem case studies today. When India's Aadhaar identity ecosystem was formed now over a decade ago, it was a bold plan to create a fully digital ID across all of India that could be utilized as a core element for digital service provision. The effort, when it began, was also unregulated, and stayed that way for some time. The lack of controls allowed abuses and significant function creep to occur.[4] India's landmark Supreme Court ruling in 2018 kept the core functioning of the Aadhaar system,[5] but the Court significantly curtailed its abuses and required additional corrections. The result was a significantly improved Aadhaar identity ecosystem.

---

[1] *The Dark Side of Identity: Mitigating the risks,* Episode 23, Segment: Mini Documentary. Interviews and narration, Pam Dixon. Editing, Mishka Orakzai. Co-produced by ID4Africa and World Privacy Forum, hosted by ID4Africa. https://id4africa.com/livecast-ep23-the-dark-side-of-identity-mitigating-the-risks/ See also: *Denied Identity in Keyna,* Video, Namati, Feb. 23, 2022. https://namati.org/news-stories/video-denied-identity-in-kenya/. See also Abdi Larif Dahir, Kenya's new digital IDs may exclude millions of minorities, Jan. 28, 2020. https://www.nytimes.com/2020/01/28/world/africa/kenya-biometric-id.html.

[2] Zack Whittaker, *A huge Chinese database of faces and vehicle license plates spilled online: Another mass data lapse exposes new weaknesses in China's sprawling surveillance state*, Tech Crunch, Aug. 30, 2022. https://techcrunch.com/2022/08/30/china-database-face-recognition/?guccounter=2

[3] For example, Kenya passed an amendment to its national ID law in 2019 that would have allowed the collection and use of DNA in its national identity ecosystem. Kenya's Supreme Court ordered a prohibition on Kenya from collecting DNA for its national ID system. Humphrey Malalo, Omar Mohammed, *Court orders safeguards for Kenyan digital IDs, bans DNA collecting*, Reuters, January 31, 2020. See also initial reactions to proposal for DNA collection: Alice Munyua, *Kenya government mandates DNA linked national ID without a data protection law*, Mozilla Blog, Feb. 8 2019. https://blog.mozilla.org/netpolicy/2019/02/08/kenya-government-mandates-dna-linked-national-id-without-data-protection-law/

[4] Pam Dixon, *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S., S*pringer Nature, Health Technology. DOI 10.1007/s12553-017-0202-6. http://rdcu.be/tsWv. Open Access via Harvard- Based Technology Science: https://techscience.org/a/2017082901/.

[5] Supreme Court of India, J*ustice K.S.Puttaswamy (Retd) vs Union Of India* on 26 September, 2018. Author: A Sikri. Bench: A Bhushan, A Khanwilkar, A Sikri, D Misra.

Today, India's Aadhaar system is one the largest and most sophisticated functioning digital ID ecosystems in the world with more than 1 billion enrollees. It is not perfect. No system is, or will be. But mandatory improvements reduced harm in India's system. For example, the centralized identity registry now has a tokenization API, among other improvements, including the potential for creating a virtual ID.[6] The back-end tokenization reduces cross-database sharing. The virtual ID generates a temporary 16-digit number that can be shared with a bank, or other service provider instead of exposing the original 12-digit Aadhaar number. These are positive improvements. In addition, Aadhaar now has more oversight, with privacy and security concerns being taken much more seriously.

Digital ID ecosystems present complex and persistent challenges, which is one reason governing policies need to be crafted and implemented prior to the installation of such systems. Currently, there is a rich range of existing policy tools and technical, administrative, and procedural controls available that can help to effectively regulate digital ID systems, reduce harms to people using that system, and still support beneficial use of the identity ecosystem. Finding the right balance here will always require ongoing attention and fine-tuning. However, some things are essential components to creating a Do-No-Harm approach.

General privacy legislation can help protect identity data from being misused for secondary or unauthorized purposes. Identity-specific legislation can help by bringing focused technical and procedural controls for the administration, management, and use of identity systems. Also essential are technical protections such as mandatory requirements for tokenization of centralized identity repositories, requirements for abundant use of encryption, and continuing oversight of the systems, with ongoing auditing and appropriate penalties for abuses and breaches.

Unless these protections are put in place properly, and are meaningfully enforced, then the risks associated with digital identity ecosystems will hold back the utilization of digitalized services. Law enforcement access to identity data is no small matter to contend with when crafting appropriate rules that find the balance between legitimate law enforcement needs and individuals' trust in the ecosystem. It is a fine balance, and a necessary one.

In the United States, we are already seeing an extraordinary chilling effect on trust in digital information ecosystems due to a 2022 Supreme Court ruling that overturned a long-recognized constitutional right for women regarding reproductive health.[7] The ruling resulted in an exodus of young women from certain kinds of health-related apps, websites, and entire digital ecosystems. The fear is that the linkage of disparate data through overlapping identity systems would create new risks to suddenly illegal reproductive health activities. The general point is that identity ecosystems, if not finely regulated and balanced, can become problematic in law enforcement contexts under some circumstances.

Aside from technical and legislative protections, an important task policy makers must consider is to create a set of international multi-stakeholder guidelines regarding digital identity ecosystems. This work needs to lead with the principle that identity ecosystems must first Do

---

[6] *Aadhaar Tokenize API, Version 1.* Unique Identification Authority of India, Government of India, 2019. https://www.uidai.gov.in/images/resource/aadhaar_tokenize_api-ver-1.0-08022019.pdf. Policy for the Aadhaar tokenization policy is contained in *Circular 1 of 2018, Implementation of virtual ID, UID token, and limited KYC*, UIDAI, https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf

[7] Jack Gillum, *Post-Dobbs America is a digital privacy nightmare*, Bloomberg, US Edition, August 4 2022. https://www.bloomberg.com/news/articles/2022-08-04/period-tracking-apps-among-common-post-dobbs-privacy-risks?leadSource=uverify%20wall

No Harm. Without that commitment, the rest of the principles may be good, but they do will not have the proper guiding star. At the end of the day, the digital identity ecosystems that are central to digitalization must in fact Do No Harm.

How can we accomplish this, practically speaking? It is my hope that the OECD, for example, would establish a process that seeks to develop digital identity principles, something akin to its formal guidance on privacy, which has influenced policy worldwide.[8] The OECD has formal multistakeholder rules in place, and this is essential to create fair and balanced guidance and ensure that all stakeholders are represented and heard. To date, there is a gap: such principles do not yet exist for all jurisdictions.

On this identity day, 2022, it is especially important to commit to improving **access to identity** and the **quality and management of identity ecosystems** in a manner consistent with the basic principle of Do No Harm. All of these goals are essential.

Credits: ID Day Graphic, courtesy of ID4Africa

Original publication date: 16 September 2022

[8] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Recommendation of the Council, 23 September 1980. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm