Giving people a 'digital identity' could leave them vulnerable to discrimination, experts warn

August 30 2019

Credit: CC0 Public Domain

Global efforts to give millions of people missing key paper documents such as a birth certificates a digital identity could leave them vulnerable

to persecution or discrimination, a new study warns.

Work is underway to use digital technology so refugees and others lacking vital legal papers can have access to services such as health and education. But this could also provide a new way for ethnic minorities to be discriminated against and marginalized by officials and governments if safeguards are not in place, according to new research.

The World Bank estimates that over one billion people currently lack official identity documents—either because they never had it, or because they have lost it—and the United Nations Sustainable Development Goals include the aim to provide legal identity for all by 2030.

Without identity documents people can have difficulty accessing many basic services including healthcare, social protection, banking or education. Asylum-seekers without documentary evidence of their identity and age may incur significant problems in acquiring legal status in a host country.

However, the University of Exeter Law School study warns digital identity could allow for more "efficient" ways to discriminate against highly persecuted groups of people such as the Rohingya minority in Myanmar, as the technology would make their ethnic minority status more visible.

Dr. Ana Beduschi, who led the research, said: "Technology alone cannot protect human rights or prevent discrimination. Depending on how digital identity technologies are designed and used, they may also hinder the rights of those that they intend to benefit. Having a digital identity may make people without legal documentation more visible and therefore less vulnerable to abuse and exploitation. However, it may also present a risk for their safety. If the information falls into the wrong hands, it may facilitate persecution by authorities targeting individuals

based on their ethnicity.

"Giving people a digital identity will only help protect their human rights if those who provide it mitigate any risks of potential discrimination and promote high standards of privacy and [data protection](#)."

Governments and initiatives run by public-private partnerships are using technology such as blockchain and biometric data from fingerprints or iris scans to provide official identification, to control and secure external borders, and to distribute humanitarian aid to populations in need.

Data stored in the blockchain is encrypted and recorded in a way which makes it challenging to delete or tamper with. Those who support the use of blockchain say this means people can own and control their own digital identity, and can then decide with whom and when to share information contained in their "digital wallet."

These schemes are not just used for those who are stateless, or lacking papers. Countries such as Estonia and India already offer citizens the chance to have a digital identity, while Australia, Canada and the UK are currently exploring ways do this.

Digital identity technology could also lead to indirect discrimination. For example, [biometric data](#) collected from older individuals are often of less good quality, so only relying on this information could lead to them experiencing obstacles in joining and using digital [identity](#) programs and accessing services.

The study warns that governments must not use [digital identity](#) information for unlawful surveillance. Any systems in place should comply with international [human rights](#) law, and have safeguards built into domestic law on data storage, duration, usage, destruction and access of third parties, as well as the guarantees against arbitrariness and

abuse.

More information: Ana Beduschi, Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights, *Big Data & Society* (2019). dx.doi.org/10.1177/2053951719855091

Provided by University of Exeter