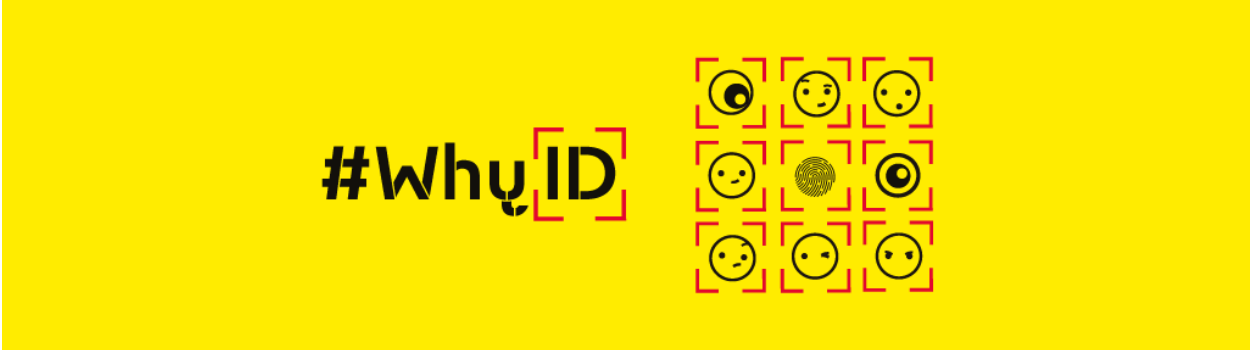


August 25, 2021

Civil society calls on international actors in Afghanistan to secure digital identity and biometric data immediately

We, the undersigned, call for an urgent safeguard of digital identity and biometric databases created in Afghanistan by development assistance missions, foreign governments previously aiding Afghan authorities, humanitarian actors, aid agencies, and the private sector vendors whose tools have been deployed to ensure they are not misused against people.

As the Taliban takes over key cities and government functions in Afghanistan, there is a tremendous fear in the country that militants and other armed actors will increasingly target human rights defenders, gender justice activists, media professionals, bloggers, digital journalists, members of the creative arts, critics of authority, and others, particularly as they gain more control over information and infrastructure that allows them to do so at scale. Several individuals and vulnerable groups have already expressed concerns about the security risks posed by their data trails.

There are at least three digital identity systems known to have been recently operational in Afghanistan: an Afghanistan Automated Biometric Identification System maintained by the Afghan Ministry of the Interior with support from the US Government; the e-Tazkira electronic national identity card system coordinated by the Afghan National Statistics and Information Authority; and U.S. military "Handheld Interagency Identity Detection Equipment" along with the biometric data it stores, which was recently seized by the Taliban. In addition, there may be several smaller biometric authentication systems and digital identity databases operated by different humanitarian agencies and other actors, including the United Nations High Commissioner for Refugees (UNHCR) collecting iris scans during refugee resettlement) and the World Food Programme (WFP) implementing biometrics in its e-voucher program.

Most international actors implemented these systems in the fragile context of Afghanistan to address security challenges and to ostensibly foster inclusion. But by embracing biometric technologies without weighing their potential for harm, these flawed systems are now putting Afghanistan's most vulnerable people in a human rights and security crisis.

The World Bank has long pushed for adoption of digital identity systems in Afghanistan, providing "active technical advice" and "financing and implementation" to the government. The Bank argued

August 25, 2021

digital identity tools would lead to more inclusion, particularly for women.[1] But now, those tools may empower the Taliban to monitor women's participation in everyday life, and even their decision to vote, putting them at heightened risk.

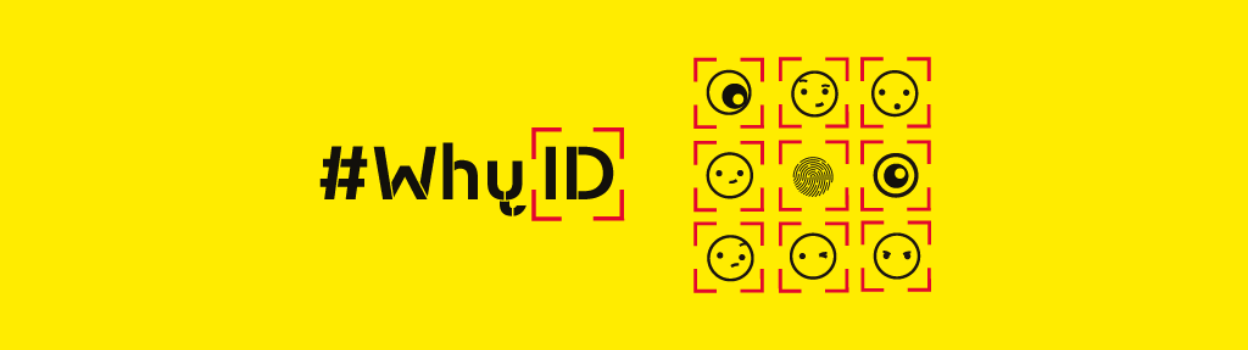
The United States military and International Security Assistance Force used biometrics in counter-terrorism operations to document a wide net of individuals of interest, ranging from anyone who may be associated with a suspected terrorist, to government officials, local contractors, people who received microloans, and more.

Humanitarian and aid agencies have also pushed for biometric databases to be used for payment of government salaries, humanitarian aid cash transfers, at madrassas (ostensibly to improve security), for issuing new business licenses, and even linked to voting as an "anti-fraud measure" during the 2019 elections. In addition, aid agencies that have hired locals often do so without the budgets to ensure their safety. Employees of foreign and humanitarian agencies have long been at risk of reprisals.

People in Afghanistan, as well as those who have fled the country as refugees, have little to no control over their participation in these systems and how they impact their lives. The databases forementioned store biographical information (including ethnicity, religion, nationality) and biometric information (fingerprints, facial image, iris), and might contain additional log information. For instance, Afghanistan's identity card, the Tazkira, is required for access to public services, to vote, for public sector employment, to register SIM cards, land and property ownership, and to obtain bank loans. The e-Tazkira was digitized in 2018, and a lot of data is linked to this record — including, controversially, ethnicity and religious belief. According to press reports, all this sensitive personal data and related information may soon come to be controlled by the Taliban or other actors seizing power within the Afghan government. In addition to the data maintained within systems controlled by or contracted to Afghan authorities, there are the databases managed by different aid agencies and humanitarian organizations. These types of databases contain sensitive information and, as privacy experts have explained, place vulnerable people in harm's way. Under authoritarian regimes, these data have been used to target vulnerable people, and digitized, searchable databases amplify the risks of abuse of this data.

These are all clear examples of why the mandatory and centralized collection of extensive data — especially biometric data — is always dangerous, and why civil society organizations from around the

[1] This article from the World Bank was publicly available as of August 18, 2021, but has since been taken down.



August 25, 2021

globe have joined the #WhyID campaign calling on international actors to think carefully about the risks and alternatives before adopting biometrics and other digital identity tools.

For all these reasons, we urge aid agencies, humanitarian organizations, and other international actors operating within Afghanistan — as well as the private sector vendors who supply and service digital identity tools — to urgently take the following steps:

1. **Wherever possible, immediately shut down systems and securely erase data.**
2. **Impose a moratorium on any continued usage of biometrics in Afghanistan without prior human rights assessments that can ensure that any such systems are safe, inclusive, not prone to error, and are the least intrusive means of authentication available.**
3. **Carefully control and audit which parties have access to data of beneficiaries and staff, including checks to see patterns of access revealing efforts to surveil and profile individuals and vulnerable communities.**
4. **Ensure there is no unrestricted access, including by suspending or disabling systems which permit access without oversight, to ensure unknown actors cannot access systems in ways that may allow them to bring individuals to harm.**
5. **Move data off computer infrastructure physically located in Afghanistan to infrastructure outside of the influence of militants and other actors seeking to intimidate vulnerable communities and at-risk individuals.**
6. **Implement data leak protections to detect unauthorized upload or transfer of data or databases.**
7. **Take remedial steps to inform anyone whose data has been compromised or who may be at risk, to support individuals who have been harmed by misuse of their data, and to ensure unintended access to an individual's data does not cause further harm.**
8. **Make public announcements of detected or known breaches of data, and provide authenticated mechanisms for individuals to verify if their personal data was included in the breach.**

#WhyID

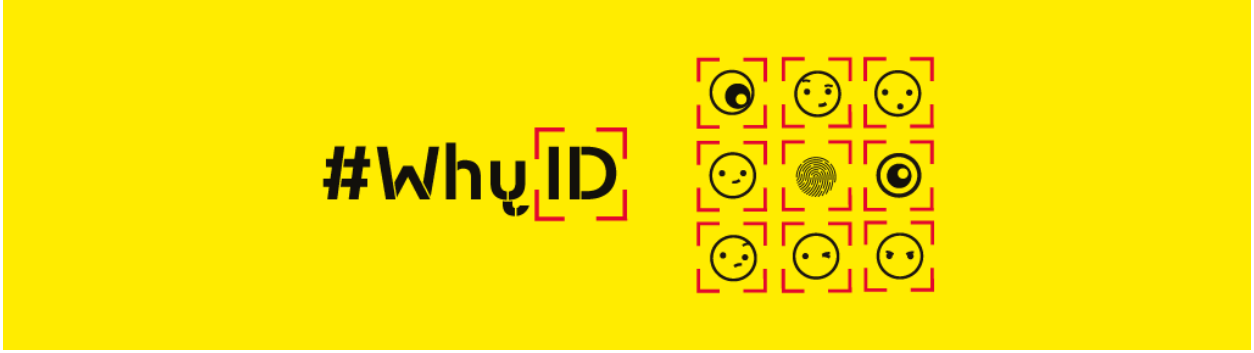
August 25, 2021

ORGANIZATIONS

Access Now
Anglican Church in America
ARTICLE 19
Association for Progressive Communications
Body & Data, Nepal
Braveheart Foundation
Commonwealth Human Rights Initiative
Digital Welfare State and Human Rights Project, Center for Human Rights and Global Justice
Electronic Frontier Foundation
European Center for Not-for-Profit Law (ECNL)
Foundation for Media Alternatives
Fundación Datos Protegidos
Fundación InternetBoliviaorg
Fundación Karisma
Global Data Justice project, Tilburg Institute for Law, Technology, and Society, Tilburg University
Hami DajuVai, Nepal
Hiperderecho (Peru)
Human Rights First
Human Rights Online Philippines (HRonlinePH)
IFEX
Impacto Digital
Instituto para la Sociedad de la Información y Cuarta Revolución Industrial (Perú)
IPANDETEC Central America
Kandoo
Manushya Foundation
Mnemonic
OPEN ASIA|Armanshahr
Queer Youth Group, Nepal
Sursiendo (Mx)
Swathanthra Malayalam Computing (SMC)
Taiwan Association for Human Rights (TAHR)
TEDIC
United Network of Young Peacebuilders (UNOY Peacebuilders)
Unwanted Witness
Usuarios Digitales

INDIVIDUALS

Anivar Aravind
Alexandra Argüelles (Mozilla Fellow)
Brandon Sullivan
Brindaalakshmi. K
Denique Soutar
Edgar Whitley
Guissou Jahangiri (Vice President, FIDH)
Jodi-Ann Quarrie
Josephine Goube (Techfugees Inclusion)
Keren Weitzberg
Margie Cheesman
Namita Kandel
Pat Walshe (Privacy Matters)
Paz Bernaldo
Pradeep Esteves
Rukshana Kapali
Timothy Reiniger (Special Advisor on Digital Identity to the Anglican Bishop of Maine)
Sanjog Thakuri
Will Byrne (Human Rights First)



August 25, 2021

For More Information, please contact:
Carolyn Tackett | **Deputy Advocacy Director** | carolyn@accessnow.org |