

Hajira Maryam, Tip Sheet

Lead Advisor on AI and Strategic Communications, Amnesty Tech, Amnesty International

Investigating Biometric Tech and Identity business: The multi-billion dollar identity industry is turning people's identities into a commodity to be extracted or traded. The rapid deployment of biometric technologies into the Global South is happening with little critical scrutiny, and the identity business is a major blindspot for investigative journalism. In this timely panel, veteran journalists dig into new technologies such as iris scans and fingerprint systems, and share practical techniques and sources for investigating biometric supply chains, large personal information databases, and the deals behind these procurements.

Overview

There are significant human rights implications associated with biometric technologies, including digital ID systems. Their implementation often results in forms of mass surveillance, where the interlinking of databases, infrastructures, and information can produce a 360-degree view of individuals.

Across jurisdictions in the Global Majority, these systems are rarely optional. Instead, they are imposed on people and communities, and the enforcement mechanisms surrounding them frequently lead to the exclusion of persons with disabilities, as well as both younger and older populations.

Governments typically justify these systems through techno-solutionist narratives. They commonly argue that digital IDs will facilitate service delivery, such as access to social benefits, education, healthcare, SIM cards, and other essential services, or that they are necessary to combat corruption and terrorism. However, those who are already marginalized and who do not fit the variables defined by the state can become targets of heightened surveillance, harassment, and control.

In most cases, digital ID systems are developed through partnerships between governments and private companies. Notably, many of these companies are not based in the countries where the projects are implemented. They may be located in the Gulf, in the EU, or elsewhere, and some EU-based firms even operate from the Gulf or other jurisdictions to evade stricter regulatory frameworks. As a result, responsibility and complicity extend beyond the Global Majority; they are also exported from the Global North into these contexts.

Alongside private companies, international financial institutions, most prominently the World Bank, play a major role in promoting these systems. The World Bank's ID4D initiative has been a central driver pushing for the expansion of digital ID infrastructures across the Global Majority.

Human rights implications of Digital ID systems

Mass Surveillance-Mission Creep: Digital ID systems are one of the key tools leading to mass surveillance. It leads to unlawful tracking of individuals, including journalists and other marginalized communities.

Disproportionate amount of data collected: These systems harness and collect vast amounts of sensitive data of individuals. This is disproportionate. The data collected is also at risk of being used for other purposes that are unlawful. Such as discriminatory policing, segregation, and curbing freedom of movement.

Exclusion: Digital ID systems are becoming mandatory to provide access to social protection measures across the Global Majority. Those who do not possess the required identification numbers are excluded from the system. Specially those who are already marginalized.

Examples

Pakistan

- **NADRA:** Nadra is the key Digital ID institution in Pakistan. It has a history of excluding communities, including trans community, and ethnic Bengalis. If you lack a digital ID in Pakistan, you are excluded from accessing essential services, including education, sim card and health care.
- [DEEP by World Bank](#) aims to accelerate the digitisation of Pakistan's economy through several measures including enhancement of the current digital ID systems, promoting financial inclusion, and enhancing citizens' access to essential government services ranging from access to education to healthcare through National Data Exchange Layer (NDEL) portals. DEEP will also expand Pakistan's mass surveillance arsenal as it will allow mass data harvesting of individuals (including their biometric data), sharing and exchange among various government databases and agencies without safeguards. This will be forcing people to unwillingly – or even unknowingly – forfeit their right to privacy. The introduction of such interconnectivity between databases, in the absence of regulation and safeguards, potentially paves the way for unknown – and unknowable – human rights abuses linked to the exploitation of personal data.
- [Amnesty International's recent investigation about the firewall system and the Lawful Intercept Management System \(LIMS\) to Pakistan](#) found how EU companies (Utimaco and Datafusion) are exporting the LIMS system to the country. The Lawful Intercept Management System (LIMS)

uses technology from the German company, Utimaco, through an Emirati company called Datafusion.

India

Amnesty Intl also published a technical explainer a last year about India's Samagra Vedika's human rights risks and its use of a technical process called "entity resolution" wherein machine-learning algorithms are used to merge databases together, with the goal of assessing the eligibility of welfare applicants and detecting fraudulent and duplicate beneficiaries in social protection programmes.

The external procurement of these systems by governments from private companies increases the barrier for civil society and journalists to investigate the technical makeup of digitalized social protection. As a result, private and public actors who are responsible for the design and implementation of these automated tools escape accountability, whereas people impacted by these systems get stuck in a bureaucratic maze, with little to no access to remedy.

Occupied Palestinian Territories

Use of FRT as a tool in this broader system of arbitrary restrictions on movement—looking specifically at the emblematic cases of Hebron and East Jerusalem, the only two cities in the OPT with Israeli settlements within their bounds. Present a non-exhaustive overview of the scale and breadth of biometric surveillance, and the human rights violations associated with these technologies, in particular facial recognition, in Hebron and East Jerusalem.

The main focus is facial recognition surveillance as carried out by the Israeli security forces, including the Israeli army operating under the Ministry of Defense and Israeli police forces under the Ministry of National Security. However, the expanding use of surveillance by settlers – at times using similar hardware –will be covered. Focus on on FRT used for identification purposes (also known as 1:n or "one-to-many"), a type of facial recognition Amnesty considers to be a technology of mass surveillance and wholly incompatible with international human rights law. The corporate actors that provide surveillance technology to the Israeli authorities include TKH Security, domiciled in the Netherlands, and Hikvision, domiciled in the People's Republic of China.

Denmark (non-Global majority example):

The way the Danish automated welfare system operates is eroding individual privacy and undermining human dignity. By deploying fraud control algorithms and traditional surveillance methods to identify social benefits fraud, the authorities are enabling and expanding digitized mass surveillance. MitID (a

digital identity system that residents in Denmark use to identify themselves to access public and private sector services).

Udbetaling Danmark (UDK-Denmarks welfare agency) has mandated a company, [*Arbejdsmarkedets Tillægspension \(ATP\)*](#), to administer social benefit and fraud control efforts. In turn, ATP has partnered with private multinational corporations, including [*NNIT*](#), to develop fraud control algorithms tailored to ATP's specifications.