Registering refugees using personal information poses risks to people giving sensitive biometric data

July 19 2023, by Joseph K. Nwankpa

Credit: CC0 Public Domain

The number of refugees worldwide reached record high levels in 2022. More than 108.4 million people have been forced to flee their homes

because of violence or persecution. Meanwhile, governments and aid agencies are increasingly using a controversial method of effectively identifying and tracking many refugees.

This method, known as biometrics, involves collecting someone's physical or behavioral characteristics, ranging from fingerprints to voice. Organizations that collect the personal physical data can store it to instantly recognize someone after scanning their fingerprints or irises, for example.

The United Nations refugee agency, often known as UNHCR, is among the groups that have grown their biometrics programs over the past several years to help identify refugees and deliver lifesaving aid and other services.

As a cybersecurity scholar, I think it is important to understand that while identifying people using biometrics might be convenient for organizations collecting the data, the practice comes with inherent privacy risks that can threaten vulnerable people's safety.

How it works

The biometrics data-gathering process begins with enrollment, which involves representatives from a government or organization collecting someone's personal physical information when they perform intake into a registration system.

Many people also routinely use biometrics for personal reasons, like recording their own fingerprints so they can unlock and use their phone.

Organizations can use this kind of personal biometric information to authenticate a person's identity—meaning, confirming that a person is who they say they are. Or, they can use it to simply identify someone and

determine who they are.

Authentication works by comparing a person's previously captured images or recordings—their biometrics—with their recently collected biometrics information.

Identification, on the other hand, compares a person's recently collected biometrics against all other people's templates stored in a biometrics database.

U.S. law enforcement and international travel-related companies alike tend to use biometrics in their work. That ranges from identifying re-offending criminals across multiple jurisdictions, for example, or quickly identifying people as they pass through an airport or cross an international border.

Cybersecurity challenges

For groups of people like refugees who might not be carrying passports or other forms of identification, biometrics provides a convenient and reliable way to verify their identities while reducing the risk of fraud.

Aid workers can also use biometrics systems in remote areas with limited cell service or internet, which is common in refugee processing centers in poor countries.

More than 80% of the refugees registered with UNHCR have a biometric record. In most cases, this is considered a standard practice that is necessary for refugees to receive aid.

In Jordan, for instance, UNHCR uses uses iris scans to identify refugees and distribute monthly allowances.

Human rights concerns

But refugees and advocacy groups alike have voiced human rights concerns, arguing that collecting refugees' biometric data can put an already vulnerable group at risk. That can happen if a militant group or government that pushed people to become refugees gets hold of their personal information and is able to potentially identify them if they are in hiding.

Unlike passwords and PIN numbers, fingerprints and facial recognition are unique and cannot be changed if there is a security breach.

Ukrainians in need of aid following Russia's invasion of Ukraine have pushed back on UNHCR and other U.N. agencies using biometrics. As a result, it has become more common there for people to be registered in other ways, such as by using their Ukrainian national tax identity numbers or their passports.

Another concern observers have made is that if a biometric database is breached, cybercriminals can take people's data and try to impersonate them and steal their identities.

Security breaches can be particularly dangerous for refugees.

Researchers at the University of North Carolina exposed flaws of compromised biometric systems in 2016 when they designed an experiment to spoof facial recognition systems. The researchers downloaded social media photos of volunteers and and used the images to construct three-dimensional replicas of faces. The 3D-developed faces successfully tricked four of the five facial recognition systems.

Things have gone wrong

Refugees and other people in vulnerable positions have experienced devastating consequences after having their biometric data breached.

For instance, the Taliban in Afghanistan seized the U.S. military's biometric collection and identification devices in August 2021 after the U.S. withdrew its final troops from Afghanistan. The U.S. collected and used this data to track terrorists and other potential insurgents.

Human rights activists expressed concern that the Taliban could use the biometric data to identify—and target—Afghans who helped the U.S. coalition forces by serving as translators and in other positions after the U.S. withdrawal.

The biometric devices, contained Afghans' biometric data, including iris scans and fingerprints.

While the Taliban have said that they will not retaliate against Afghans who had worked with the U.S. and other Western coalition forces, the U.N. has tied reports of civilians and Afghan soldiers being executed to compromised U.S. biometrics databases.

Similarly, in 2021 news reports revealed that the U.N. shared its biometric data of more than 800,000 Rohingya refugees living in Bangladesh with the government there. The Bangladeshi government then shared the information with the Myanmar government—the same government that Rohingya refugees feared would hurt or kill them.

The U.S.-based advocacy group Human Rights Watch reported that the U.N. had informed Rohingya refugees that they needed to give their biometrics information in order to receive lifesaving aid and other services from the U.N. Some people interviewed in refugee camps said that they went into hiding after they learned that their information had been shared.

A need for reform

I believe that there is a need to consider whether and how refugees are giving consent for the recording of their personal information—and whether refugees are fully informed of the inherent risks associated with biometric system use.

At a minimum, I think that UNHCR and other groups collecting biometric data information should set up stronger security models and undertake routine cyber risk assessments to understand evolving threats.

Without the necessary money and technological ability to respond to cyberthreats, U.N. agencies and others will remain vulnerable to cyberattacks, which can undermine people's rights and ability to find safe refuge.

Provided by The Conversation