Societal Benefits vs Privacy of Biometric ID

This article explores the societal benefits of biometrics vs privacy/data security concerns.

One of the key priorities under the German Presidency of the Financial Action Task Force (FATF) from July 2021 to June 2023 is to harness the potential of technology for the digital transformation of relevant Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) measures and practices.

Digital ID or biometric ID is clearly one tangible pathway for such a transformation. Biometric ID allows for more efficient and effective customer due diligence (CDD).

What do we mean by biometric ID? The Cambridge dictionary defines biometrics as referring to detailed information about someone's body, such as the pattern of colour in their eyes that can be used to prove who that person is. Biometrics therefore could include facial, retina, fingerprint, and voice print etc. When referring to biometrics, there is really no need to mention ID, as it is inherent in the definition.

Biometric technology has already transformed aspects of our lives – for the better. For example, travellers witness the convenience and efficacy of e-Passport as travellers enter and exit national borders based on their biometrics. It is quick and secure although at this stage travellers still have to carry their physical passports. Besides, many smart phone users and users of internet or mobile accounts are using biometrics to log into their accounts online.

By using biometrics, it is possible to confirm individuals' identities based on "who they are," rather than by documentation - "what they have" - or passwords - "what they know." These authentication factors can also be combined ("multifactor authentication") to gain higher levels of security.

Biometrics makes it hard for someone to forge your ID document, and you cannot really forget or lose your biometric identity, unlike for passwords! Go to the so-called "dark web" and people can easily sell passwords, passports and driver licence details, but not people's biometrics. How many occasions have you read about people giving their passwords and personal details in response to email phishing or the passwords of people who have been hacked?

However, there are lobby groups opposing the use of biometric technology because of privacy and data security concerns. They have argued that there are too much risks and adoption should therefore be delayed or limited. These concerns should not be ignored and they need to be addressed in order for the full societal benefits of biometrics to be reaped.

There are concerns raised that biometrics could be abused and used for nefarious purposes. That risk is true, but that is not a valid argument against the use of the

technology. The human race has done an effective job in abusing privacy and freedom without biometric technology. There are many traditional means for such purpose in terms of physical appearance, name identification and cultural recognition.

The issue is not the technology per se, it is about the user of the technology. Basically, it is not the technology that should be the primary focus – but the regulatory and technological frameworks which should exist to ensure that societal benefits are maximised and inappropriate use is minimised.

There is also confusion between biometrics used for ID authentication and biometrics used for recognition. ID authentication is either "match on server" and/or "match on device." Either approach allows the user to voluntarily agree to share one's biometrics for e-KYC purposes. It is a convenient, compliant and secure means of proof of identity.

This should not be confused with biometric recognition where your face or fingerprints are matched against the data in a server, and you have not given prior consent. Biometric recognition's goal is to discover someone's identity, such as law enforcement procedures which involves checking the biometrics of a person to determine whether that person is on a criminal watch list. Even in this scenario, the societal benefits are clear.

The European Union's Global Data Protection Rule (GDPR) is the gold standard in privacy and data protection. It establishes the right to be forgotten (right to erasure: individuals have the right to request for erasure of their personal data), and the clear requirement for consent and severe penalties for failure to comply with the Rule which came into force in May 2016. The Rule has applied to around 500 million EU citizens and long-term residents irrespective of where they reside globally.

The GDPR states that the consent must be explicit before the collection of the data and the right to withdraw his or her consent must be retained at any time. With the exception of the right to be forgotten, none of those principles are inconsistent with AML/CFT standards. The right to be forgotten must be balanced with the AML/CFT record keeping requirements.

There are many countries globally that have adopted biometric technology for ID authentication purposes. For example, the Unique ID Authority of India Aadhaar program provides a unique identification number for the nation's 1.34 billion citizens by using biometric means. The aim is to use the program as an identification framework for various government schemes and provide financial inclusion for socially disadvantaged citizens. Aadhaar allows for e-KYC by reporting entities and service providers for AML/CFT.

Its neighbour, Pakistan, has the National Database & Registration Authority (NADRA). It has transformed the paper-based ID management to a state-of-the-art identity system with back-end data input and reporting. From paper to computerized cards and finally

chip-based cards with advanced security features, NADRA covers Pakistanis residing within and outside of the country.

NADRA is the back rock for the country's e-KYC system for individuals – either as the direct customer, authorised representative of a company, natural person trustee or the beneficial owner of a company or discretionary trust.

In Africa, the ID4Africa Movement is driven by the need to establish identity-for-all, not just as a legal right, but also as a practical necessity to enable inclusive digital access to services in Africa. ID4Africa believes that service-oriented identity ecosystems built on the respect of privacy and human rights are essential for growth of digital economies and will become even more crucial as African countries move to implement the provisions of the African Continental Free Trade Agreement (AfCFTA).

Adopting biometric technologies have proven to simplify customer onboarding process. Biometrics and document identity scans have shown to be the most promising tools so far and are popular among customers and financial institutions as an alternative to traditional paper-based CDD processes.

There is also growing evidence that biometrics is conducive to financial inclusion. It has been reported that 13% of the world's population does not have any ID documentation, according to ID4D Global Dataset by World Bank last published in 2018. Biometrics provides a platform for inclusion in the formal financial sector because it is easier and less costly for socially marginalised and disadvantaged communities to be on board. The benefits are not limited to financial inclusion but also obvious for social and health programmes.

Finally, as mentioned in earlier articles, biometrics are imminently suited to the world as COVID-19 has led to unprecedented global challenges, human suffering and economic disruption. The demand and benefits of contactless biometrics are obvious.

Biometrics does not mean that it is the only option of digital or non-digital ID. People may decline to provide their biometrics because of religious or other reasons. They have the right to choose not to avail of the convenience and efficacy of biometrics – just as some people choose not to fly but instead select land or marine transport, even when the cost is not a consideration.

In conclusion, it is not that there are no privacy and data protection issues with biometrics – but no more or less than paper-based ID systems. Arguably, the societal benefits of biometric ID outweigh the risks, as long as best practice principles like the GDPR are adopted, such as explicit consent and right to remove biometric records as long as it does not violate other applicable laws such as record keeping under AML/CFT laws and relevant standards.

Alliance for Financial Stability with Information Technology
August 2021