UPHOLDING THE RIGHTS OF CHILDREN:
SPECIAL CONSIDERATIONS ON THE USE OF BIOMETRICS IN IDENTITY SYSTEMS

Written by Ann Livingston, Kristen Wenz and Nicola Richards

IDENTITY SYSTEMS AND DEVELOPMENT

A comprehensive civil registration and identity management systems is key to unlocking development potential in the modern world. In high income countries, civil registration systems coverage is universal and provides the foundation from which other identity systems are built. On the other hand, across low and middle-income countries substantial investments are made in developing, digitizing and sustaining costly, parallel identity systems while civil registration systems remain neglected, despite the potential for cost savings by the state and independence from externally developed, parallel monitoring mechanisms. Data generated from civil registration systems are the primary source of vital statistics needed for demographic data (disaggregated by geographic area, sex and age), required for good governance, planning, and measuring progress towards over 70 targets for the Sustainable Development Goals.

The use of biometrics recognition in functional or legal identity systems have provided a promising way to authenticate or uniquely identify a person. However, biometrics alone do not prove an individual's identity, and therefore should be linked to a legal identity document. Whereas a significant number of countries have introduced biometric and digital identity systems for adults, children are often excluded and left behind.

BIOMETRICS, CHILDREN AND IDENTITY

Children who were never registered at birth make up more than half of the global identity gap (650 million, ages 0-16)[1]. In Sub-Saharan Africa only 1 out of 4 newborns have a birth certificate and there has been little improvement in birth registration coverage for the continent for nearly two decades. Children without a birth certificate have no legal proof of their identity or family ties which is essential for proving or re-establishing a child's identity.

The validity for use of biometric technologies has been established for adults – however, there is less certainty on the use case, accuracy or recallability of biometric technologies for young children. When systems fail to reliably capture or authenticate a child's biometrics, and a child does not have a birth certificate there is a high risk for exclusion. Considerations for implementing biometric recognition in identity systems outside of the adult population requires understanding the best interests of the child. Considerations such as if the use of particular types of biometric recognition for children is ethical, if appropriate safeguards are in place to ensure a child's biometric data will be protected, and if there are alternative solutions or approaches that could be deployed which come with less risk.

EMERGING TECHNOLOY & OPPORTUNITIES

Biometric recognition via well-established technology continues to make rapid advancements in proving accuracy and reliability (particularly on fingerprints, irises and facial images), there has not been a solution to date that has been able to overcome the challenges of capturing a single reliable biometric from infant to age five, to adulthood and old age. Promising new technologies and innovative solutions are emerging, such as using parent's biometrics to link to a child's birth certificate, the use of machine learning to capture the rapidly changing biometrics of young children are continuing to emerge. To date, several technologies have been designed to capture newborn biometrics, they lack longitudinal evidence beyond one year, and often require the use of costly devices which are less appropriate or viable for use in low income or in low resource settings. As advances in technologies for child recognition have only been made in recent years, there is limited evidence or guidance available on their use.

TECHNOLOGICAL GAPS

Technological challenges and gaps have concrete impacts on children's lives. Data protection is also at risk as data can be tracked, misused, or released to unauthorized parties, encroaching on children's' right to privacy. Skin condition – sweaty or dry skin – as well as environment conditions - humidity, temperature or light exposure - in which the biometric traits are being taken can have a direct impact on the system's efficiency to capture high-quality biometrics. There are two major factors that affect the recognition accuracy of biometric systems: age of the person at enrolment, and the time lapse between enrolment and query. These are referred to as the 'age' and 'ageing' affects, and while not unique to children, their impact is much more pronounced due to the double interaction of age and ageing that children face.

The age effect accounts for variations in recognition accuracy between different user groups based on their age at enrolment and is largely influenced by how easy or difficult it is to acquire a given biometric trait, and the impact this has on template quality. For example, the skin of newborns is prone to drying and peeling soon after birth, distorting the impression process for print-based modalities. The ageing effect relates to variations in recognition accuracy due to an increase of time between enrolment and query; and isn't necessarily related to physical features of the biometric trait, but the ability for the technology to acquire and recognize physical structures over time. As children undergo drastic growth in the first period of their life are particularly impacted by the ageing effect. Other risks include fundamental technology limitation (signal to noise limits) related to the capture and matching of a child's biometrics. This issue can lead to incorrect verification with "false rejects" – when the user is wrongly rejected from the system or inversely "false accepts" – when an identity in incorrectly recognized into the system, for example when the biometric traits are matched with another person's identity.

---

[1] Alan Gelb and Anna Diofasi Metz. 2018. Identification Revolution: Can Digital ID be Harnessed for Development?

UPHOLDING CHILDREN'S RIGHTS

Children are a vulnerable population and therefore require a focused assessment of the risks and benefits of biometric recognition technologies for the protection of their rights. Ethical and social considerations with regards to the use of biometric data are directly related to the right to protection of personal data. Children's right to identity, starting from birth, to protection, and privacy are often referred to as main challenges to the ethics of child biometric identification.

Convention on the Rights of the Child

- Article 7: every child has the right to a name and to be registered at birth.
- Article 8: every child has the right to an identity, and for their identity to be preserved
- Article 16: every child has the right to privacy and protection.

When system failures occur such as failure to enroll, or a false rejection, it raises the risk of exclusion as the burden of proof (that is, proving the system is at fault, and not the user) falls on the user in question, who is more likely to be from disadvantaged groups, including children. Other risks associated with the use of biometrics in children include a restricted view of family.

In other words, the use of biometrics will not necessarily be pertinent for separated children whose caretakers are usually not their immediate family. Additionally, specific protection is required to the process and use of sensitive data which reveals certain personal characteristics of individuals. Biometric data and information on individual upon which people could be identified based on specifics and distinguishing signs have the potential to make children vulnerable to discrimination.

THE NEED FOR ADDITIONAL RESEARCH

The use of biometrics in children is at its early ages and while it undoubtedly contributes to ensuring the uniqueness of an individual through a secure authentication factor, it still raises legal, ethical and social concerns that ought to be addressed to ensure children's rights are being fully protected. Yet, as of today, there is insufficient evidence to back up the use of biometrics with children in general, but they there is clear and conclusive evidence on the effect of age and ageing on matching performance accuracy of biometric recognition systems, with significantly poorer performance among the youngest age groups. More research is needed for understanding the use of biometrics on children and the urgent need for more appropriately-designed/ child centered technology. There is need for clearly defined policies and procedures around the protection of data in order to guarantee children's rights are upheld, including additional focus from the identity community to ensure every child has a birth certificate.