DATA PROTECTION BY DESIGN AND BIOMETRICS IN HUMANITARIAN ACTION

OBJECTIVES

The main objective of this working session is to explore practical measures that can reduce the risks related to the processing of biometrics data in humanitarian action. The goal is to come up with a list of such measures.

To achieve this, it is proposed to explore two orthogonal but complementary dimensions:

Assessing Proportionality: What are the potential mechanisms to assess the proportionality of using biometrics to provide a mean of identifying? How could we properly balance the theorical benefits with reality of the field? *(Note: underlying to this question is the further question of whether those benefits really exist but this fundamental point should not be the focus of the session).*

Designing for Purpose Limitation: If biometrics is deployed, what technical means can be included in the design of the solution to tackle the problem of being over-purposed by nature? The principle of purpose limitation should guide the reflection which is intended to be quite technical. Properties of irreversibility, revocability, and unlinkability will also play a role in the reflection.

The panel will address these dimensions, while the roundtable discussion will be structured more as a workshop, addressing foundational questions to aid humanitarian actors in deciding if and when biometric data is truly necessary and proportionate for identification purposes, as well as the choices that need to be made to design a system which maximizes the mitigation of the risks.

BACKGROUND INFORMATION

BIOMETRICS

The purpose of collecting biometrics, as its Greek roots indicate ('bio' meaning 'life', and 'metrics' meaning 'measure'), is to measure a parameter of life. In other words, biometric data relate to who we are and provide the measure of a particular trait of an individual. Whenever an organization collects biometric data, it is with the intention to identify people.

In humanitarian action, the need to identify individuals has always been crucial to deliver aid. Whether to provide adequate health treatment or in forensic science, humanitarian workers rely on the ability to identify affected people. In practice, this means that lists or databases of individuals are created. These lists can contain records of personal information, including biographic data (e.g., names, sex, marital status, origin, data of birth), identity numbers referencing other lists (e.g., national id, voter id, tax id) and biometric data.

The use of biometric-based identification systems in humanitarian programs is not a novel concept and many humanitarian organizations have invested substantially into the development and deployment of biometric solutions as a mean for facilitating individual registration, authentication, and aid distribution. By replacing paper-based systems, biometrics promise improved accountability toward affected communities and donors,

reduced fraud and aid diversion, and increased efficiency and effectiveness in humanitarian programmes.

However, despite these promises, the use of biometrics-based identification systems in humanitarian has sparked significant debate and concern over potential misuse and risks, often viewed as part of "humanitarian experimentation"[1]. Documented abuses and specific risks related to biometric data collection have led to calls to limit or even ban such systems. Parallelly, other studies highlight cases where biometrics have facilitated aid distribution and helped to reach objectives otherwise complicated to achieve.

Interestingly, a comparison between successful and more problematic biometric deployments reveals that they often rely on nearly identical technical components. Most biometric identification systems share common designs and data flow structures, utilizing the same foundational methods to process raw biometric data and generate templates for database storage, regardless of the specific solution deployed. Likewise, the algorithms used to compare templates (whether matching two or more templates) are frequently similar across different systems. This shows that the potential for harm in a biometrics-based system may hinge less on the technology itself and more on external factors such as context, scale, and governance.

The importance of context does not come as a surprise, as it is often said that the risks posed by technology stem not only from the technology itself but from how it is applied. However, implementing a system that incorporates a well-defined threat model and adheres to Data Protection by Design (DPbD) practices can mitigate certain risks associated with processing biometric data.

DATA PROTECTION BY DESIGN AND PURPOSE LIMITATION

A Data Protection by Design and by Default approach ("DPbD") refers to an approach to technology development that proactively considers and mitigates data protection risks, to ensure that data protection is not an afterthought but an integral feature of the system's architecture. Article 25 of the GDPR defines DPbD as a manner of designing systems that addresses the risks to the rights and freedoms of individuals posed by data processing activities, taking into account the likelihood and severity of those risks. DPbD principles in humanitarian contexts may include, for instance, decentralized architectures that keep sensitive information on the user's device, encryption to secure data flows, and anonymization techniques that obscure sensitive information during processing.

In the case of biometric data, applying DPbD is particularly important because of the inherent sensitivity and "over-purposing" potential of biometric traits. Purpose limitation, a core principle in data protection, is critical in this context. Biometric traits often carry more information than required for identification; for instance, an iris scan may reveal health conditions, a face scan might imply ethnicity, gender, or age, and DNA data can provide extensive information about an individual's characteristics. Additionally, biometric data is unique and non-renewable — unlike passwords or IDs, we have only one set of fingerprints or irises. Consequently, once our iris scan is in one database, it is in all databases!

GUIDING QUESTIONS

- What are the risks related to the use of biometrics in humanitarian settings?
- How can the practice of DPbD be leveraged to help humanitarian organizations overcome such risks?
- What are the current obstacles that may prevent DPbD from being incorporated into the working modalities of organizations that rely on biometrics?

[1] See "Humanitarian Experimentation", https://blogs.icrc.org/law-and-policy/2017/11/28/humanitarian-experimentation/ and Engine Room & Oxfam "Biometrics in Humanitarian Sector", https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf

- Due to the nature of biometrics (i.e. revealing a lot of personal information, permanent), perhaps the best mitigation is to enforce purpose limitation, what does it mean in practice?

ADDITIONAL MATERIAL

- Massimo Marelli, eds. "Chapter 8 Biometrics." In *Handbook on Data Protection in Humanitarian Action*, 3rd ed., 127–42, 2024. doi: https://doi.org/10.1017/9781009414630
- Graf Narbel Vincent, Sukaitis Justinas, "Biometrics in humanitarian action: a delicate balance", International Committee of the Red Cross, https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/
- Sandvik, Kristin Bergtora, Katja Lindskov Jacobsen, and Sean Martin McDonald. "Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation." *International Review of the Red Cross* 99, no. 904 (April 2017): 319–44. doi:10.1017/S181638311700042X
- The Engine Room. "Biometrics in the Humanitarian Sector: A Current Look at Risks, Benefits and Organisational Policies," July 2023. https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf