Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
ICRC response to White House Office of Science and Technology Policy Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

January 2022
Prepared by
Laura Walker McDonald, Senior Advisor, Digital Technology and Data Protection
International Committee of the Red Cross (ICRC) Regional Delegation for the United States and Canada

Descriptions of use of biometric information for recognition and inference

Many humanitarian organisations have experimented with the use of biometric identification in recent years.¹ This development is the subject of much debate²; but is in part the result of increasing pressures to improve the accuracy and cost-effectiveness of aid delivery, and to know more about recipients of aid.

The ICRC is committed to working at the cutting edge of technology, where doing so enables the organisation to better conduct its activities, and help people affected by conflict. The ICRC has long been using biometrics in limited use cases, for example in forensics and the restoration of family links, and by putting fingerprints on the travel documents it issues. The organisation uses DNA profiling to help identify human remains to determine the fate of the missing, and is employing facial recognition technology to help people find their family members.³

However, the ICRC’s role requires it to also be alert to the potential risks of technology for affected populations. For example, the ICRC has raised concerns relating to the military applications of certain emerging technologies, in particular autonomy,⁴ AI and machine learning.⁵ The ICRC sees the protection of personal data whose disclosure could put its beneficiaries at risk, or otherwise be used for purposes other than those for which it was collected, as an integral means of preserving its

---

neutrality, impartiality, and independence, as well as the exclusively humanitarian nature of its work. The organisation has sought to highlight data protection challenges in humanitarian action through its Data Protection Framework\(^6\) and ‘Digitharium’ public events series.\(^7\) As such, the ICRC has set limits on the uses and management of biometric data – for example, not retaining fingerprint information in any database – and has published a Biometrics Policy.\(^8\)

Within those limits, ICRC is exploring the potential to expand its use of biometrics in carefully considered ways.

Humanitarian aid organisations like the ICRC are under pressure to provide aid to as many people as possible, in a global context of growing numbers of crises, of increasing severity, and shrinking aid budgets. Humanitarian needs often surpass available resources. If we can ensure that each person receives only their fair share of aid, and that the people who receive aid are the people our programs planned to reach, we are better able to make the best use of our budget and help as many people as possible. In a humanitarian context, this is not an easy challenge: many individuals are unable to prove who they are, or are part of a marginalized group, whose private information is of extreme sensitivity. Often, aid recipients are given a card and a pin code or a password, but these can be forgotten or lost, or stolen and used by another person.

Biometric identification systems in aid programmes could allow us to ‘identify’ and/or ‘deduplicate’ aid recipients, to ensure that each person receives the right kind and amount of aid, without requiring them to have or show other forms of identification. See page 7 below for more information about the research and development we are conducting.

**Exhibited and potential harms of a particular biometric technology:**

Biometric data is extraordinarily powerful. It creates a permanently identifiable record of an individual – an individual cannot renew or change their biometric identifiers. It is also over purposed by nature: a rich set of data points which is more than what is required for authentication\(^9\).

“Function creep”

Every biometric sample can reveal a lot about the data subject – for example, an iris scan can reveal some health conditions, and facial or voice recognition may reveal ethnicity, age or gender. This kind of ‘function creep’ is difficult to prevent at collection, opening up the possibility that the data will ultimately be used in ways that aid recipients do not want, understand or consent to. The data protection principles of purpose limitation and data minimization cannot, therefore, be respected. Such rich and personal information poses a unique risk mitigation challenge, because as technology develops, new capabilities and new purposes might be found for the data. This means that risk analysis and mitigation practices, and ethical and practical policies, need to plan for risks and purposes that have not been identified yet.\(^10\)

---


\(^7\) ICRC (undated), *Digitharium*, available at https://www.icrc.org/en/digitharium, accessed 01/14/22


\(^10\) See for example Oxfam comments during the Digitharium debate on biometrics, linked at note 1 above.
**Misidentification:** Biometrics are also not infallible, particularly in humanitarian crisis contexts where populations often differ from the test subjects used to develop such technologies. For example, while exploring the potential of facial recognition technologies to aid in reuniting families with their loved ones, the ICRC was confronted with recurring racial, gender and age biases of several facial recognition algorithms, leading to both false negative and false positive results. Families can open a tracing request for a missing person with the ICRC or with a national Red Cross and Red Crescent Society, like the American Red Cross. They provide information about the missing person, including photographs. In this context, facial recognition could enable case workers to more easily identify possible matches across large databases. While none of this process is automated and humanitarian experts are always ‘in the loop’ to use their judgement about whether or not the match is likely to be correct, one can imagine the distress a wrong match could cause to an already suffering family.

**Data retention, transfer and proliferation**

Humanitarian organizations are under implicit – and at times, explicit - pressure from donors, which are increasingly demanding “end-to-end auditability”, and making more-and-more humanitarian funding contingent on demonstrable anti-fraud and accountability processes, to explore biometrics technology. Though donors usually stop short of explicitly requiring the use of biometrics, such systems appear to offer – and are certainly marketed as – the most attractive means of satisfying multiple humanitarian programming requirements. Biometrics are also playing a central role in the scaling up of cash-transfer programming across the sector, with many financial service providers viewing them as a correspondingly simple way to meet to meet their KYC (Know Your Customer) and other legal ‘due diligence’ requirements. Both of these modalities imply that some data is retained and/or shared with authorities. Increasingly, humanitarian organizations are complying with this trend.\(^{11}\)

For the recipients of aid this can be problematic. In various large-scale humanitarian contexts, affected populations have expressed serious concerns about the use of biometrics and potential access to the data by non-humanitarian organisations, particularly for security and migration control.\(^{12}\) Because biometric data is attractive for these purposes, humanitarian organisations can be requested or required by States to disclose it. They are also vulnerable to cyber-operations by State and non-State actors seeking unauthorized access. In some cases, such as was recently reported in Afghanistan, biometric datasets gathered by non-humanitarian actors could be compromised, handed over or otherwise obtained by non-state armed groups or a new authority during a transition of power. This data could subsequently cause harm to those individuals.\(^{13}\)

---


\(^{12}\) See, for example, the Reuters article describing protests in Yemen, above at note 2

Given the permanent and sensitive nature of the data, and the known challenges for governmental and non-governmental organizations of keeping such data secure over long periods of time, for a donor to require the collection of biometric data runs counter to the do no harm principle. And given that the humanitarian landscape is often confusing for communities and recipients of aid, the collection and subsequent handover of such sensitive data by one humanitarian actor can have knock-on effects for trust and humanitarian access for all actors, however principled their action.

**Conclusion – Data Protection and Limited Collection:** All actors, including States, must consider the eventualities outlined above in exploring and implementing biometrics technologies and develop comprehensive contingency plans, including for remotely removing or destroying the data at short notice. The best way to defend such sensitive data, however, may be not to collect it in the first place. The ICRC recommends limiting collection of biometric data to that which is strictly necessary, and implementing procedures for data subjects to be able to request removal from the database and measures to protect data subjects whose biometrics have been compromised. The ICRC Policy is available to other actors to use as a resource and a template.

For these reasons, the ICRC has ruled out, for the present, storing biometric data in a centralized location. We are exploring ways to convert biometric data into a second data value that cannot identify individuals, be reverse engineered to reveal the original record or combined with another dataset to reveal a person’s identity.

**Exhibited and potential benefits of a particular biometric technology:**
Biometric identifiers are always with us, in some cases including after death, barring some physical changes due to accidents or, in rare cases, alteration to those traits by choice. They do not require a high degree of literacy to use. As noted above, in a humanitarian emergency, biometrics can be a powerful form of personal identification, not requiring government-issued documentation. This makes it more inclusive, and can reduce risk by allowing individuals to be identifiable as their physical selves, and not linked to an administrative record – so, done well, they can protect privacy in cases where biographic data is extremely sensitive. Some biometric traits, such as palm and finger veins, may not be machine-readable from a distance, preventing some unwanted scanning.

For authentication purposes, biometrics may be one of the only mechanisms that guarantees that the bearer of the credential is the one who was given the credential (e.g. unlike pin or password which can be used by somebody else).

**Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case:**
Legal and regulatory basis for use of biometrics, and the ICRC biometrics policy
Biometric data are recognised as sensitive in both law and practice. The EU’s General Data Protection Regulation (GDPR) – which has galvanised jurisdictions across the world into adopting, revising, proposing or considering their own data protection laws – designates biometrics as “special

---

category” data, bringing higher thresholds for both collection and protection of the data.\textsuperscript{15} The African Union \textit{Convention} on Cybersecurity and Personal Data Protection,\textsuperscript{16} the “modernised” Council of Europe \textit{Convention} on the Automatic Processing of Personal Data,\textsuperscript{17} and many national privacy laws also contain special rules restricting the processing of biometric data. Although these rules do not apply to the ICRC, which has adopted a Data Protection Framework that reflect its status as an international organisation, the core principles upon which they are based are the same.\textsuperscript{18} In its Handbook on Data Protection in Humanitarian Action, and through its Biometrics Policy,\textsuperscript{19} the ICRC fully recognizes the risks introduced by the collection and processing of biometrics data. We strongly believe that protecting data is really about protecting people and if a biometrics-based identification system is designed and deployed without properly applying the fundamental principles of data protection - such as minimizing data collection and retention, purpose limitation, and privacy by design - the risks will outweigh the benefits.

The ICRC Biometrics Policy, adopted by the ICRC Assembly in August 2019, was elaborated over an 18-month period and is the result of extensive research, analysis, consultation and reflection. This process included a review of all situations and scenarios in which the ICRC is processing or considering the use of biometrics, an evaluation of the “legitimate basis” and specific purposes for the processing, and the identification of organisational, technical and legal safeguards.

Establishing a legitimate basis is straightforward where the ICRC processes biometric data in accordance with specific objectives associated with its mandate – for example to identify individuals in its work on Restoring Family Links and determining the fate or whereabouts of the missing – and where particular objectives cannot be realised without using biometrics. In this case the ICRC processes the biometric data as a matter of “public interest” (in the implementation of the ICRC’s mandate).

The issue is much more challenging when it comes to using biometrics for beneficiary management and aid distribution, where the processing of the data may not be viewed as an integral part of an ICRC mandate-based activity requiring the identification of individuals. Because the purpose here is primarily linked to efficiency, and insofar as aid can be (and long has been) distributed without the need for biometrics, the ICRC would have to establish that the “legitimate interest” it has in establishing any biometric identity management system does not outweigh the potential impact on the rights and freedoms of the individuals concerned. This balancing test is typical in data protection law whenever a data controller relies on their own interests as a basis for processing.

\textbf{Token-based systems – a balance?}

In its analysis the ICRC found that there was, however, a balance that could be found that would still allow the institution to leverage the advantages that biometric authentication offers in respect to efficiency and effectiveness and ensuring end-to-end accountability in its aid distributions, while minimizing the risks to which its beneficiaries would be exposed.


\textsuperscript{18} See above at note 6

\textsuperscript{19} See above at note 8
This balance rests on operations wishing to use biometric data in the registration and verification of beneficiaries limiting the processing to a token-based system. In practice this means that beneficiaries may be issued with, for example, a card on which their biometric data is securely stored, but that the ICRC will not collect, retain or further process their biometric data (and will not therefore establish a biometric database).

The token/card may be used to verify beneficiaries during aid distributions to ensure that the aid reaches those individuals for whom it has been earmarked, but no other use of the biometric data will be possible. If the beneficiary wants to withdraw or delete their biometric data, all they will need do is return or destroy the card. If authorities seek to compel humanitarian organisations in a particular country to hand over the biometric data of beneficiaries, the ICRC will not face such pressure because it will not in fact have this type of data. This solution allows the ICRC to leverage the benefits of biometrics for the purposes of authentication, but not for deduplication, because we can never review our databases for duplicate biometric records.

The organisation continues to participate in research and policy discussions to help drive innovation and industry standards. At present, standards around system interoperability to prevent vendor lock-in, or accountability for performance, are lacking. The revised ISO standard 24745 on ‘Biometric Information Protection’, due to be published in early 2022, will be a step in the right direction, as would national and supranational regulation like those under discussion for artificial intelligence.

The role of consent
While the ICRC is committed to rendering its data processing as transparent as possible to aid recipients and affected populations, it does not believe that consent provides a legally valid basis for data processing in many emergency situations.

This is because consent to data processing cannot be regarded as valid if the individual has no real choice: for example, where the provision of aid is effectively dependent on the provision of personal information, and consent is therefore unlikely to be “freely given”. In addition, the power imbalance and situation of the beneficiary means that there is no real “choice”, and the individual is induced to accept what is proposed by a humanitarian organisation. Moreover, where biometrics are concerned, it is extremely difficult to ensure that consent is genuinely “informed”, since in many situations the affected population may not be able to fully comprehend the technology, information flows, risks or benefits that underpin the processing of their biometric data.

The Biometrics Policy, in line with the ICRC Rules on Personal Data Protection, requires the ICRC to explain the basis and purpose of data processing to its beneficiaries, including any data-sharing arrangements, regardless of the basis for the processing. The ICRC also seeks to ensure that beneficiaries have the opportunity to ask questions and object to data processing if they so wish, particularly where data may be shared with third parties. If people do not want to provide their biometric or other personal data, or to see their information shared for humanitarian purposes with partners, the ICRC will respect their wishes.

No data sharing for non-humanitarian purposes
The Policy also makes it clear that the ICRC will only use biometric data where it enhances the capacity of the organisation to implement its humanitarian mandate and will under no circumstances share biometric data with third parties, including authorities, that may use them for non-humanitarian purposes. Even where exclusively humanitarian grounds for sharing biometric data can be identified, strict conditions must still be satisfied before the data can be transferred by the ICRC.
The Future, Research and Development

Further to that, the ICRC is committed to the advance of research in the domain of “secure biometrics”. In practice, raw biometrics samples (images) are processed before they can be used for authentication. This process of extracting the “features” generate a binary version of the biometric trait which is called a biometric template. It is only in this format that a search for matches can be performed, and this often involves a probabilistic comparison (e.g. “the match is 99.3%”). These templates are still very sensitive and personal data and various attacks can be performed against them. For instance, templates can be reversed to reveal the raw biometrics, or templates in two different systems are so similar that they reveal they are linked to the same individual. Last but not least, many systems use templates that are as unique and permanent as the raw biometrics meaning that they cannot be revoked and renewed if compromised.

These biometrics templates must be protected and there are several research approaches like biometrics crypto systems (i.e. where the biometrics is used as the cryptographic key) or cancellable biometrics. Unfortunately, very few commercial actors are actively investing in them and we intend to launch partnerships projects in this area.

About the ICRC

The International Committee of the Red Cross (ICRC) is an impartial, neutral, and independent humanitarian organization working to save lives and protect people in hotspots around the globe. We work with Red Cross and Red Crescent Societies worldwide to deliver relief and protect people from armed conflict and violence. The ICRC is independent from the UN system.

Our work is strictly humanitarian: to assist and protect people affected by armed conflict and violence, ensuring that their basic needs are met. Respect for the law of armed conflict saves lives and limits damage to civilian property, which helps prevent displacement.

Established in 1863, we have worked with states, including the US government, for over a century to develop and apply the law of armed conflict – rules that protect soldiers, civilians, detainees, and the wounded and sick in war.

Find out more about the ICRC at icrc.org.