Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases

Ben Hayes (AWO agency, Consultant legal advisor to the ICRC)
Massimo Marelli (Head of the ICRC Data Protection Office)

The International Committee of the Red Cross (ICRC) works with some of the most vulnerable people in the world, providing humanitarian assistance to populations affected by armed conflict and other situations of violence.[1] Like many other humanitarian organizations, the ICRC is exploring new technologies to support its operations and beneficiaries. As part of its digital transformation agenda, the ICRC developed a Biometrics Policy ("the Policy") that both facilitates the responsible use of biometrics and addresses data-protection challenges. ICRC adopted the Policy in August 2019,[2] which recognizes the legitimacy and value of using biometrics to support its programmatic and operational objectives while also ruling out the creation of any central, biometric databases in the short term. This article discusses some of the factors brought to bear on the decision-making process we went through as an institution.[3]

1 International Committee of the Red Cross, "The ICRC's Mandate and Mission," https://www.icrc.org/en/mandate-and-mission.

2 International Committee of the Red Cross, "The ICRC Biometrics Policy," October 16, 2019, https://www.icrc.org/en/document/icrc-biometrics-policy.

3 This article builds on Ben Hayes and Massimo Marelli, "Facilitating innovation, ensuring protection: the ICRC Biometrics Policy," ICRC, *Humanitarian Law & Policy*, October 18, 2019, https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy.

BIOMETRICS IN THE HUMANITARIAN SECTOR

The ICRC works in more than ninety countries and is part of a global humanitarian network of over eighty million people.[4] It provides healthcare, food, basic shelter, clothing, access to education, employment, and assistance to detained persons, and also helps restore family links by reuniting separated persons and finding missing persons. To address the logistical challenges of protection and assistance programs, some humanitarian organizations use biometric identification systems to enroll people in humanitarian programs and verify their identity when providing services or assistance. The primary justification for this use is that recipients of humanitarian assistance frequently lack identity documents, which poses a challenge if they need to be identifiable.

Humanitarian organizations have intensely debated when and how people "need" to be identifiable, and the legitimacy of using biometrics to perform that function.[5] On one side, continuity of healthcare and some forms of humanitarian assistance clearly need people to be identifiable (e.g., for provision of travel documents or financial services). For example, the United Nations Refugee Agency (UNHCR) has a clear mandate to identify refugees and asylum seekers, and to provide them with identity documents[6] (though it has been heavily criticized for deploying biometrics[7]). However, most humanitarian organizations do not have a formal mandate to provide people with an identity or supporting documentation. They have primarily developed and implemented biometric ID systems because of the perceived efficacy and accountability gains such systems provide.[8]

While existing ID cards, social security numbers, and other documents may be used by humanitarian organizations to check or verify an individual's identity, these cannot be unequivocally associated with a single individual in the way that a biometric ID can. Biometric databases can also be used to prevent the same individual from registering in an aid program more than once, which is attractive for humanitarian organizations that are concerned about individuals or families obtaining more assistance than has been earmarked for them.[9] Indeed, biometrics have played an increasingly large role in the scaling up of cash-transfer programs (CTPs).[10] For financial service providers that are obligated to verify the identity of account holders

4 ICRC, "The International Red Cross and Red Crescent Movement," https://www.icrc.org/en/who-we-are/movement.

5 See, for example, "Head to Head: Biometrics and Aid", *The New Humanitarian*, July 17, 2019, https://www.thenewhumanitarian.org/opinion/2019/07/17/head-head-biometrics-and-aid; and Katja Lindskov Jacobsen, Kristin Bergtora Sandvik, and Sean Martin McDonald, "Humanitarian Experimentation," ICRC, *Humanitarian Law & Policy*, November 28, 2017, https://blogs.icrc.org/law-and-policy/2017/11/28/humanitarian-experimentation/.

6 United Nations High Commissioner for Refugees, "Note on the Mandate of the High Commissioner for Refugees and His Office," *Refworld*, October 2013, https://www.refworld.org/docid/5268c9474.html. Note: The ICRC also issues emergency travel documents, albeit very few by comparison.

7 See for example Chris Burt, "UNHCR Reaches 7.2M Biometric Records but Critics Express Concern," Biometric Update, June 24, 2019, https://www.biometricupdate.com/201906/unhcr-reaches-7-2m-biometric-records-but-critics-express-concern.

8 The Engine Room and Oxfam, "Biometrics in the Humanitarian Sector," March 2018: https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf.

9 Laura Gordon, "Risk and Humanitarian Cash Transfer Programming: Background Note for the High Level Panel on Humanitarian Cash Transfers," *Overseas Development Institute*, May 2015, https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9727.pdf.

10 See, for example, World Bank Group, "Guidelines for ID4D Diagnostics," 2018, http://documents1.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf. Cash and other forms of direct financial disbursement are widely viewed as providing beneficiaries of humanitarian programs with more dignity and autonomy than food parcels and other disbursed goods, but donors are concerned that these programs are more susceptible to fraud and abuse.

and cash recipients, biometric data could offer a simple and straightforward way to meet multiple operational needs and legal obligations.[11]

These are crucial issues for humanitarian staff, who want operations to be as efficient as possible, and to ensure that scarce humanitarian services and assistance are provided to intended recipients. There is also implicit pressure to use biometrics from donors, which increasingly demand "end-to-end auditability" (allowing the tracking of humanitarian funds from donor to recipient) and make funding contingent on anti-fraud and accountability processes. All of this has contributed to a tangible impetus for humanitarian organizations to use biometrics for beneficiary registration and aid distribution. And why not, if everyone else is doing it?

RISKS AND CONCERNS

Concerns about the use of biometrics in the humanitarian sector are well known, but are often overlooked.[12] Biometric data are unique, immutable, and create a permanently identifiable record for individuals in vulnerable humanitarian contexts who may not want to be identifiable forever. The creation of a permanent biometric record underpins concern that this record could increase the risk of harm to the persons concerned in the event it was subsequently accessed by or provided to the regime or non-State actor they had fled.

Biometrics constitute particularly sensitive data[13] due to the potential for reuse or misuse, as well as "function creep," i.e., the possibility that biometrics may be used in a new way, separate from the original purpose and without the understanding or consent of the affected individuals. For example, biometrics could be shared with non-humanitarian organizations or governments for non-humanitarian purposes, such as security and migration control.[14] This is particularly concerning when biometric identity management systems are developed during a crisis or

---

11 These assumptions also dovetail with the UN's Sustainable Development Agenda, which mandates the provision of legal identity to all and targets increased financial inclusion, tacitly encouraging States and the financial sector to predicate both on a biometric identity. See, for example, Sustainable Development Goal (SDG) target 16.9: "By 2030, provide legal identity for all, including birth registration: Promote just, peaceful and inclusive societies." Financial inclusion is a target for eight of the seventeen SDGs. United Nations, Department of Economic and Social Affairs, Sustainable Development, "The 17 Goals," https://sdgs.un.org/goals.

12 See, for example, Gus Hosein and Carly Nyst, "Aiding Surveillance," *Privacy International*, October 2013, https://privacyinternational.org/report/841/aiding-surveillance. See also Katja Lindskov Jacobsen, "On Humanitarian Refugee Biometrics and New Forms of Intervention," *Journal of Intervention and Statebuilding* 11, no. 4 (2017): 529–551, https://doi.org/10.1080/17502977.2017.1347856.

13 The General Data Protection Regulation (EU) 2016/679 (GDPR), for example, introduces a general prohibition against the processing of biometric data unless, inter alia, the data subject has given their "explicit consent" (something which is problematic in a humanitarian context, as discussed further below); the processing is subject to a specific law or legal agreement; the processing is necessary to protect the vital interests of data subjects who are physically or legally incapable of giving consent; or where the processing is necessary for reasons of public interest and subject to adequate measures to protect the interests and safeguard the fundamental rights of the data subject (Article 9). The recently adopted "Modernised CoE Convention 108+" on data protection broadly adopts the same approach to biometric data as the GDPR by classifying them as "sensitive data" and imposing core restrictions and conditions on their processing. The African Union Convention on Cybersecurity and Personal Data Protection also imposes restrictions on the processing of biometric data.

14 Affected populations have expressed serious concerns about the use of biometrics and potential access to the data by non-humanitarian organizations. See, for example, Aziz El Yaakoubi and Lisa Barrington, "Yemen's Houthis and WFP Dispute Aid Control as Millions Starve," Reuters, June 4, 2019, https://www.reuters.com/article/us-yemen-security-wfp/yemens-houthis-and-wfp-dispute-aid-control-as-millions-starve-idUSKCN1T51YO; "Rohingya Refugees Protest, Strike Against Smart ID Cards Issued in Bangladesh Camps," *Radio Free Asia*, October 26, 2018, *https://www.rfa.org/english/news/myanmar/rohingya-refugees-protest-strike-11262018154627.html*; and "Over 2,500 Burundi Refugees in Congo Seek Shelter in Rwanda," *Voice of Africa News*, March 8, 2018, https://www.voanews.com/africa/over-2500-burundi-refugees-congo-seek-shelter-rwanda.

emergency, where data could be used in ways that recipients of humanitarian assistance do not want, understand, or consent to. Humanitarian databases may, for example, be integrated or made interoperable with other social registries or national ID systems run by development or government partners. Technology may also advance to allow biometric profiles to be used to ascertain additional information about the data subject—for example regarding their health, ethnicity, or genetic makeup.

States have shown increasing interest in biometrics to monitor the movement of populations and identify security "threats." In December 2017, the UN Security Council called for the enhanced use of biometric ID systems to identify terrorist suspects, mandating all UN Member States to "develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law."[15] Some humanitarian organizations have already come under pressure from States to disclose biometric data for non-humanitarian purposes, though these requests are generally not in the public domain. Organizations are also vulnerable to cyber-operations by State and non-State actors seeking unauthorized access to their data.[16]

Biometric data use was a central theme at the 33rd International Conference of the Red Cross and Red Crescent, held in December 2019.[17] To safeguard the independence, neutrality, and trust in humanitarian organizations, the Conference adopted a landmark resolution on "restoring family links while respecting privacy."[18] Founded on the principle of purpose limitation, the resolution "urges States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement."[19]

RATIONALIZING BIOMETRICS AT THE ICRC

Prior to the adoption of its biometrics policy, the ICRC was already employing 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 (but not into any database). In addition to using DNA profiling

15 UN Security Council Resolution 2396, adopted December 21, 2017 under Chapter VII of the UN Charter on "Foreign Terrorist Fighters." As the UN Special Rapporteur for the Protection and Promotion of Human Rights While Countering Terrorism has stated, the biometrics mandate provided by the Security Council is "deeply concerning" because the Resolution does not contain any explicit reference to constitutional or legislative protections for privacy or data protection. See Fionnuala Ní Aoláin, "The UN Security Council, Global Watch Lists, Biometrics, and the Threat to the Rule of Law," *Just Security*, January 17, 2018, https://www.justsecurity.org/51075/security-council-global-watch-lists-biometrics/.

16 Massimo Marelli, "Hacking Humanitarians: Moving towards a Humanitarian Cybersecurity Strategy," ICRC, *Humanitarian Law & Policy*, January 16, 2020, https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/.

17 International Federation of Red Cross and Red Crescent Societies, 33rd International Conference, 2019, https://rcrcconference.org/about/33rd-international-conference/.

18 Reuniting families separated by conflict and disaster is a core activity of the International Red Cross and Red Crescent Movement globally. See "Restoring Family Links While Respecting Privacy, including as it Relates to Personal Data Protection" (33IC/19/R4), 33rd International Conference of the Red Cross and Red Crescent, December 9–12, 2019, https://rcrcconference.org/app/uploads/2019/12/33IC-R4-RFL-_CLEAN_ADOPTED_en.pdf.

19 Ibid., Article 11.

to help identify human remains to determine the fate of the missing, the ICRC is exploring facial recognition technology to locate persons sought by family members following separation due to humanitarian emergencies.[20]

This is part of a broader ICRC strategy to transform and adapt its humanitarian response by seizing the opportunities that new technologies offer its operations and beneficiaries. Managing the attendant risks is central to this digital transformation agenda.[21] Early in 2018, following significant interest in expanding biometric data use, the ICRC Directorate requested an assessment of the operational, ethical, and reputational risks involved, as well as an institution-wide policy that would facilitate both innovation and data protection.

ICRC developed the policy over an eighteen-month period that included extensive research, analysis, consultation, and reflection. ICRC reviewed all scenarios in which the ICRC processed or considered the use of biometrics, evaluated the "legitimate basis" and specific purposes for the processing, and identified organizational, technical, and legal safeguards. Although the ICRC is not bound by national or regional data-protection law, it has adopted similar rules that require it to identify a legitimate basis (equivalent to a legal basis) for all of its data-processing activities.[22]

In some cases, ICRC's rationale for biometric data use was straightforward: for instance, when used with specific objectives associated with its international mandate and where particular objectives cannot be realized without using biometrics. Examples include using DNA to determine the fate or whereabouts of the missing, or using facial recognition to match missing and sought persons in its work on restoring family links.[23] In these cases, the ICRC processes the biometric data as a matter of "public interest."[24] Subject to appropriate safeguards, biometric data processing provides the ICRC with tools that greatly enhance its capacity to implement its mandate with respect to persons separated or missing in humanitarian emergencies.

Other cases are much more challenging: for example, when the potential use case involves biometrics for beneficiary management and aid distribution, where requiring the identification of individuals may not be viewed as an integral part of an ICRC mandate-based activity. Because the purpose is primarily efficiency, and aid can be (and long has been) distributed without the need for biometrics, the ICRC determined that the "legitimate interest" of using a biometric identity-management system did not outweigh the potential concerns over rights and freedoms. This balancing test is typical of data-protection laws (e.g., as in GDPR), whenever a data controller relies on their own interests as a basis for processing.[25]

---

20 See "Rewards and Risks in Humanitarian AI: An Example," ICRC, *Inspired*, September 6, 2019, https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificial-intelligence/.

21 In addition to "doing no harm," ICRC maintains principles of impartiality, neutrality, and independence. The protection of personal data that could be misused or whose disclosure could put its beneficiaries at risk is an integral means of ensuring these principles are upheld. See ICRC, "The Fundamental Principles of the International Red Cross and Red Crescent Movement," https://www.icrc.org/sites/default/files/topic/file_plus_list/4046-the_fundamental_principles_of_the_international_red_cross_and_red_crescent_movement.pdf.

22 See ICRC, "Rules on Personal Data Protection," ("ICRC Rules"), https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection. The rules were adopted by the Directorate of the ICRC on February 24, 2015 (updated on November 10, 2015), and updated and adopted by the ICRC Assembly on December 19, 2019.

23 ICRC, Restoring Family Links, https://familylinks.icrc.org/en/Pages/home.aspx.

24 ICRC Rules, Article 1.

25 ICRC Rules, Article 1; GDPR, Article 6.

After careful consideration, ICRC concluded that it was possible to leverage the efficiency and effectiveness gains of biometric authentication, as well as end-to-end accountability in its aid distributions, while also minimizing the risks to its beneficiaries. This balance rests on using biometric data in beneficiary registration and verification, and limiting the processing to a token-based system. In practice, this means that beneficiaries could be issued 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 therefore not establish a biometric database).

The token/card could 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 will be possible. If the beneficiary wants to withdraw or delete their biometric data, they may return or destroy the card. If authorities seek to compel humanitarian organizations in a particular country to hand over the biometric data of beneficiaries, the ICRC will not face such pressure because it will not have the data.

KEY FEATURES OF THE POLICY

Adopted by the ICRC Assembly in August 2019, the ICRC Biometrics Policy sets forth staff and program roles and responsibilities,[26] the legitimate basis for processing biometric data by the ICRC,[27] the specific purposes and use cases for which the use of biometrics is authorized, [28] and the types of biometric data that may be processed by the ICRC.[29] Specifically, it allows the ICRC to:

- include the fingerprints of the holder on travel documents issued by the ICRC to persons who have no valid identity papers, enabling them to return to their country of origin or habitual residence or to go to a country which is willing to receive them;
- use biometric identification systems to restrict access to strictly confidential information and/or mission-critical resources such as servers and control rooms in ICRC premises;
- use fingerprints, facial scans, and DNA to identify human remains recovered from disaster or conflict zones or in connection with other situations of violence;
- use digitized photographs for the purposes of tracing and clarifying the fate of separated or missing persons;
- use biometric data to ascertain the identity or fate of specific individuals in the course of investigations related to the abduction of, or attacks upon, ICRC staff members;
- on a case-by-case basis, where it has been determined that it is in the best interest of the persons concerned, collect biological reference samples for the purposes of DNA profiling to facilitate family reunification or to determine the fate of a missing person; and
- use biometrics to provide beneficiaries with a token-based verification credential such as a card that can be used to verify their receipt of those services, where the token is held solely by the Data Subject.

26 ICRC Biometrics Policy, Article 4.
27 Ibid., Article 5.
28 Ibid., Article 6.
29 Ibid., Article 7.

There are additional caveats:

- The use of fingerprints for travel documents remains limited to ink prints on hard-copy documents (with no further biometric processing by the ICRC permitted).
- Delegations may not use biometrics for routine premises control (only specific assets that require a high level of security and where profiling is limited to staff authorized to access them).
- DNA profiling for family reunion purposes is strictly limited to cases where proof that two persons are actually related is required under national law or policy.

The Policy also expressly rules out the creation of biometric databases with respect to the authorized use cases. Finally, where ICRC programs or delegations wish to process biometric data pursuant to an authorized use case, they must first conduct a data-protection impact assessment and ensure that detailed data protection by design and by default requirements are implemented as the process or system is developed.[30]

The Biometrics Policy also addresses some other common data-protection challenges, including "consent," which humanitarian organizations have traditionally sought from the people who use their services or receive assistance. In some contexts, like medical treatment, these processes have been quite robust. In others, however, people have routinely signed "consent forms" or provided a thumbprint in lieu of a signature (e.g., for those unable to write; as part of its biometrics review, the ICRC is also putting an end to this practice). "Informed consent" in data processing is subject to high standards: the ICRC Rules on Personal Data Protection require "freely given, specific, informed indication of his or her wishes by which a Data Subject signals agreement to the Processing of Personal Data relating to him or her."[31]

While the ICRC is firmly committed to transparency, it does not believe that consent provides a legally valid basis for data processing in many emergency situations. 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, power imbalances may imply no real "choice," and individuals may be induced to accept what is proposed by a humanitarian organization. Where biometrics are concerned, it is extremely difficult to ensure that consent is genuinely "informed," since affected populations may not be able to fully comprehend the technology, information flows, risks, or benefits that underpin biometric data processing.

The Biometrics Policy requires that the ICRC explain the basis and purpose of data processing to its beneficiaries, including any data-sharing arrangements, regardless of the basis for the processing.[32] The ICRC also seeks to ensure that beneficiaries have the opportunity to ask questions and object if they wish, particularly where data may be shared with third parties.[33] If people do not want to provide their biometric or other personal data, or share their data with

30 Ibid., Articles 10 and 11.
31 ICRC Rules, Definitions: "Consent."
32 ICRC Biometrics Policy, Article 18. This is in line with the ICRC Rules on Personal Data Protection.
33 Ibid., Article 18.4.

partners, the ICRC will respect their wishes.[34] The ICRC will only use biometric data where it enhances the capacity of the organization to implement its humanitarian mandate.[35]

Finally, under no circumstances will the ICRC share biometric data with third parties, including authorities, that may use them for non-humanitarian purposes.[36] Even where exclusively humanitarian grounds for sharing biometric data can be identified, strict conditions must be satisfied before ICRC will transfer any data.[37]

The ICRC will review the Biometrics Policy at least every three years,[38] including the decision not to establish biometric databases for the purposes of identity management. ICRC will review developments around the availability, security, cost, effectiveness, and impact of biometric technology, and may amend the Policy to widen the scope for using biometrics, or to introduce new safeguards.

LESSONS LEARNED

During its deliberations, the ICRC considered the option of not adopting a biometrics policy and leaving decisions about how and when to use these data to programs, operations, and delegations in the field. This option was rejected as "high risk on the basis that it could undermine, *inter alia*, the rights of the ICRC's beneficiaries, the 'do no harm' principle, and ICRC's reputation." While the internal organizational debates have been challenging, the Policy has provided much needed clarity and operating procedures for staff who were struggling to balance the perceived benefits and risks of specific uses.

ICRC consulted internal staff and external stakeholders in order to answer questions around operational needs, data-protection requirements, technology options, ethics, and risk appetite. Case-by-case assessment of the existing and possible use cases was fundamental in shaping the ICRC Biometrics Policy. However, ICRC faced many challenges because it was already using biometrics, and the new Policy could have led to changes in practice or prohibitions against certain processing options or operations. Finally, the ICRC Biometrics Policy benefited from considerable dialogue and investment in innovative compromises such as the token-based solution, which might not have been achieved through a less coherent or constructive exercise. As biometric data use-case law and data-protection enforcement actions continue to expand, the need for humanitarian organizations to develop proactive policies only becomes more important.

34 Ibid., Articles 19 and 20.
35 Ibid., Article 6.1.
36 Ibid., Article 14.
37 Ibid., Article 15.
38 Ibid., Article 21.