

The Risks of Using Biometrics in the Humanitarian Sector

Data **Surveillance** as the Price of **Survival**?

Assessing Risks and Benefits from
the Gaza Humanitarian Foundation Case



Palestinians receiving aid at one of four of the Gaza Humanitarian Foundation distribution sites

Photograph by Ahmad Salem (2025)

URL <https://www.newyorker.com/news/q-and-a/an-inside-look-at-gazas-chaotic-new-aid-system>

By Sara Albakri

Table of Contents

1. Introduction

1.1 Background

1.2 Context

2. Benefits and risks in the humanitarian sector

2.1 Benefits

2.2 Risks

3. Why is this important now?

4. The case of the Gaza Humanitarian Foundation

5. Key recommendations and Opportunities for Change

5.1 Data protection

5.2 Accountability concerns

1. Introduction

Using biometric technology in the humanitarian sector has long been a polarising topic of debate amongst aid organisations and donors. Some actors praise it as a more efficient way to streamline aid to the correct beneficiaries, while others flag risks around collecting and storing vulnerable groups' sensitive data. The question is:

How can the humanitarian sector better protect beneficiaries from the risks of biometrics?

1.1 Background

The background to this question relates to increasing pressure within the humanitarian sector to solve global humanitarian needs with technological solutions. In June 2025, 117 million people were forcibly displaced, entering 2026 with 239 million in urgent need of humanitarian assistance¹. This has forced humanitarian sectors to turn towards technological solutions to innovate faster, cheaper and efficiency driven tools. One of which has been biometric technology. Biometrics are the measurement of human characteristics such as iris and facial scans. They have been used to facilitate cash based distributions, and verify identities through database identifications. With biometrics' increased use in response to rising humanitarian needs, concerns over its risks are sometimes overlooked by technosolutionist hype, mostly from international donors. This policy brief intends to highlight the risks associated with increasing use of biometric technologies in the humanitarian sector, raising concerns on issues related to data sensitivity, consent, and state surveillance. It highlights the Gaza Humanitarian Foundation (GHF) as a recent application of extractive biometric systems, tracing its negative repercussions, and proposing a few solutions which could help mitigate these risks and effectively protect beneficiaries data rights. These suggestions contribute to wider efforts by international NGOS, such as Oxfam², to build safer humanitarian biometrics in the future.

1 Context

Biometric technology in humanitarian aid is used to digitally collect human physical or behavioural traits to facilitate the registration and authentication of aid recipients. These include recording iris scans, fingerprints and facial recognitions, which form a digital identity. Biometric technology has been increasingly recognised as efficient methods for aid distribution within the humanitarian sector over the past two decades. For example, in 2016, the UNHCR committed to expand the use of biometrics in refugee registrations,

¹United Nations, "Crisis and Emergency Response," *Global Issues*, accessed April 20, 2026, <https://www.un.org/en/global-issues/crisis-and-emergency-response>

²Zara Rahman, Carly Nyst, and Paola Verhaert, "Biometrics in the Humanitarian Sector," *The Engine Room*, March 15, 2018, <https://www.theengineroom.org/biometrics-in-the-humanitarian-sector/>

pledging to open 75 operations globally by 2020³. As of 2023, the UNHCR expanded to 90 operations reliant on biometric registrations, citing reduced management costs as a driving reason⁴. Since then the use of biometric technologies has expanded including, biometric ID's for voter registration, and cash based intervention. Two of the largest administrators of refugees, UNHCR and WFP, include biometric registries to keep track of their beneficiary transactions. For example, the UNHCR developed PRIMES, its Population Registration and Identity Management Ecosystem to categorise and store refugee biometrics⁵. The wide application of biometric technologies in key humanitarian organizations offers certain benefits as listed below.

2. Benefits and Risks of Biometrics in the humanitarian sector

2.1 Benefits

The possible benefits of Biometric technologies include,

1. **Verification.** Biometrics can help verify if an individual is who they claim to be, by comparing physical biometrics with the digital identity's recorded biometrics, reducing the risk of identity fraud. This ensures every beneficiary gets the correct amount of aid.
2. **Streamlined transactions.** Where cash- based assistance has become a more popular donation than providing food or shelter, biometrics can help make fund distributions more transparent. This helps keep organisations accountable for responsible aid distribution.
3. **Gain recognised legal status.** Building a digital identification system supported by biometric evidence can help displaced populations secure a recognised legal status. Having this legal status makes them eligible for healthcare access, education or banking services, services they would have been excluded from without formal registration⁶.

2.2 Risks

While there are certain benefits to using biometric technologies in aid delivery, it's important not to overlook the many risks. When life-saving aid is conditional on submitting your biometric data the question of whether meaningful consent can really be granted is vital. Particularly considering the fact that biometrics can seem invasive and a violation of private physical boundaries for some marginalised groups. This is one of several harms caused by humanitarian biometric technologies, these include:

³ Quito Tsui and Elizabeth Shaughnessy, "Technocolonialism and Biometrics: Reinvigorating the Call to Decolonise Aid," *Forced Migration Review*, 2024.

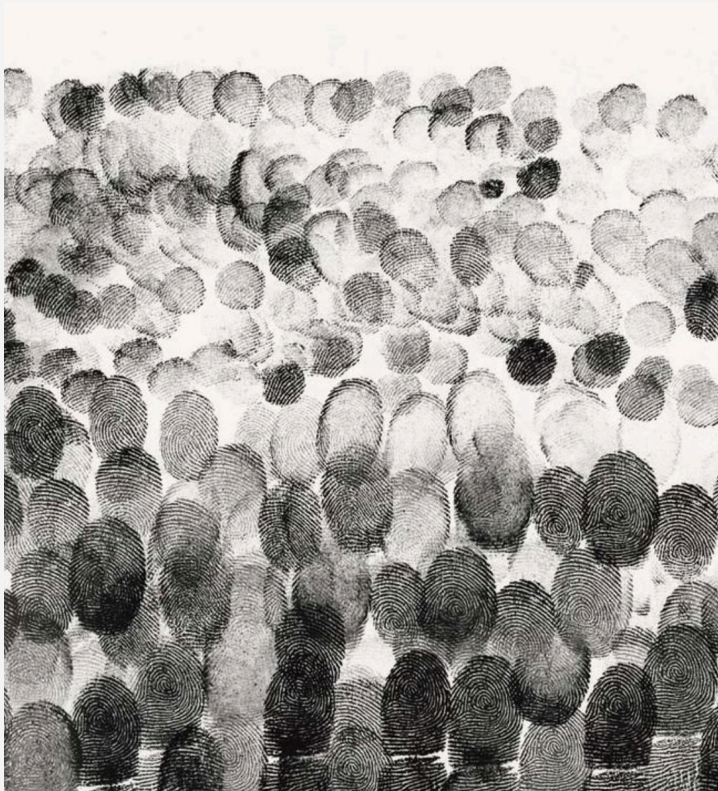
⁴ibid

⁵ Elliot Prasse Freeman, "Nothing to Lose but Their (Block)chains: Biometrics, Technoimaginaries, and Transformations in Rohingya Lives," *American Anthropological Association*, 2022.

⁶ UN High Commissioner for Refugees, "Biometrics," *UNHCR Blogs*, accessed April 20, 2026, <https://www.unhcr.org/blogs/?s=biometrics>

1. Function creep. Biometric data is often characteristics which are unique and identifiable only to the individual (ie DNA sample). The collection of permanent biometric data is risky and could cause ‘function creep’; which is where data collected for one purpose is used for different purposes without the dataholder’s consent⁷. The long term storage and easy ways to share biometric data means it could be used for tracking or profiling, creating long term risks which cannot be undone. This is in contradiction with the code of ethics enshrined in global research and practice with vulnerable communities⁸, protecting data confidentiality.

1. **Consent.** Refusal to submit biometric registration could mean refusing registration to receive aid entirely. If this is the only way to achieve aid, vulnerable individuals are not offered a choice. This does not give beneficiaries any real rights over their biometric privacy. This again, is in contradiction with the Belmont Report’s principle of justice for beneficiaries involved in activity. The lack of an opt out option leaves room for the manipulation of vulnerable beneficiaries, which violates humanitarian commitment to priority fairness and equity.



@inesberzosa, “DNA thumbprint congregation” Pinterest, 2025, <https://pin.it/1x28nRTFw>

3. Why is this important?

While discourse over biometric technologies in the humanitarian sector has been ongoing since the early 2000’s, there are pressing factors which make reemphasizing their risks even more important. These include a number of issues that have become strikingly apparent such as humanitarian biometric data being used to train state-led facial recognition surveillance. This is important because these technologies actively target and profile vulnerable populations. The very same data collected to try and enhance humanitarian aid, could be used to target and persecute those same beneficiaries:

⁷Bert-Jaap Koops, “The Concept of Function Creep,” *Law, Innovation and Technology* 13, no. 1 (2021): 29–56.

⁸ Namely Beneficence- articulated in the Belmont Report U.S. Department of Health and Human Services, “The Belmont Report,” *Office for Human Research Protections*, accessed April 20, 2026, <https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html>

1. **Private Investments in developing biometric technology.** Private company partnerships in the humanitarian sector have become large funders of humanitarian work, particularly in pressuring the integration of technology. This risks approaching humanitarian aid as a place for profit and technological innovations, rather than prioritising humanitarian relief. For example, the 45 million dollar partnership between UNWFP and Palantir technologies, was established to advance biometric software development⁹. This sought to build sensors such as iris scanning, heartbeat pulses, voice recognition and emotion detection to create a more comprehensive digital verification system for aid recipients¹⁰. This private investment in building humanitarian biometrics exists alongside Palantir's current 1.3 billion dollar partnership with the US department of defense to develop AI and automated weapons¹¹. Involving private military investors' in developing humanitarian biometrics introduces risks of clashing military and humanitarian principles.
2. **Humanitarian biometrics and State Surveillance.** Governments can request humanitarian biometric data and repurpose it for national security intelligence. The ease of circulating and analysing biometric data amongst hostile host countries or countries of origin, introduces risks of tech surveillance. This places displaced people directly in danger, especially if they are fleeing persecution and their biometric data is handed to the government they are fleeing from; As was the case with UNHCR sharing Rohingya refugees biometric data to the Myanmar government which they had fled from¹². Wider concerns are supported by other examples. The US funds UNHCR, one of the largest humanitarian organisations deploying biometrics, with an interest in its data¹³. It demands the UNHCR shares sensitive data of refugees which have crossed the US border. Seekers who are denied asylum and resettlement, have their biometric data permanently stored in the US database¹⁴. Biometric data collected for aid delivery could extend beyond humanitarian distribution, to private funders and state surveillance. Data collected for humanitarian purposes, is increasingly used by ICE to support deportation programs and to train facial recognition technologies¹⁵. This shared data is actively used to locate and prosecute marginalised groups¹⁶. In an age where data surveillance powers national security efforts, collecting highly sensitive biometric data becomes a risk in itself. Particularly considering the amount of private and

⁹Mirca Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises," *Social Media + Society* 5 (2019): 1–13, <https://doi.org/10.1177/2056305119863146>

¹⁰ibid

¹¹"Palantir (PLTR) Lands \$1.3B ...," Yahoo Finance, accessed April 20, 2026, <https://finance.yahoo.com/news/palantir-pltr-lands-1-3b-213719986.html>

¹² Mirca Madianou, "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises," *Social Media + Society* 5 (2019): 1–13, <https://doi.org/10.1177/2056305119863146>

¹³Quito Tsui & Elizabeth Shaughnessy, *"Technocolonialism and Biometrics: Reinvigorating the Call to Decolonise Aid"* (Forced Migration Review), 2024

¹⁴ibid

¹⁵Priya Morley, "AI at the Border: Racialized Impacts and Implications," *Just Security*, June 28, 2024, <https://www.justsecurity.org/97172/ai-at-the-border/>

¹⁶ibid

international funding poured into developing these technologies, which makes donors seemingly entitled to access the sensitive data collected.

3. **Biometric technologies are tested out in the humanitarian field.** With greater privatised interest in funding the development of biometric technologies, funders need a space to test these new innovations. Conflict afflicted zones have weaker data protection requirements and therefore offer an unregulated laboratory for stakeholders to try out new humanitarian technologies. This means new, perhaps insufficiently developed technologies are tested in collecting vulnerable populations' biometric data.

4. The Case of the Gaza Humanitarian Foundation:

The Gaza Humanitarian Foundation (GHF) use of biometrics to deliver aid is a strong and recent example of the technology's risks to data surveillance and privacy. At the peak of a 3 year genocide and mass starvation due to restricted humanitarian access, this case stands out as an exploitative model for humanitarian biometrics, and should not set a precedent in other humanitarian contexts. This policy brief intends to highlight the harms which emerged from the GHF's use of biometrics drawing out policy recommendations to ensure these harms are not reproduced in future uses.

Biometric scheme

In July 2025 over 100 NGOs warned of mass starvation¹⁷, shortly following the Israeli government's three month blockade on all aid supplies into Gaza¹⁸. The GHF was launched in response to this, delivering aid through biometric registration screening, militarised zones and drone surveillance¹⁹. The biometric scheme registered beneficiaries under a numerical ID to collect aid. It required sensitive data to be submitted, including photographs, fingerprints, and voice samples²⁰. These are provided in exchange for receiving food earlier than if beneficiaries were to collect aid from the GHF's militarised aid distribution points²¹. These aid distribution hubs became highly dangerous for

¹⁷Irene Pietropaoli and Sara Razai, "Privatised Food Delivery in Gaza and Violations of International Humanitarian Law," *British Institute of International and Comparative Law*, July 24, 2025, <https://www.biicl.org/blog/115/privatised-food-delivery-in-gaza-and-violations-of-international-humanitarian-law>

¹⁸TRIAL International, "Human Rights and Legal Organizations Warn Privatized 'Humanitarian' Operators in Gaza of the Risk of Legal Liability for Complicity in Serious Violations of International Law," June 23, 2025, <https://trialinternational.org/latest-post/human-rights-legal-organizations-warn-privatized-humanitarian-operators-in-gaza-of-the-risk-of-legal-liability-for-complicity-in-serious-violations-of-international-law/>

¹⁹Irene Pietropaoli and Sara Razai, "Privatised Food Delivery in Gaza and Violations of International Humanitarian Law," *British Institute of International and Comparative Law*, July 24, 2025, <https://www.biicl.org/blog/115/privatised-food-delivery-in-gaza-and-violations-of-international-humanitarian-law>

²⁰Skyline International for Human Rights, "Biometrics for Food: A Dangerous Shift from Humanitarian Relief to Coercive Surveillance", May 15, 2025, https://www.skylineforhuman.org/admin/storage/files/shares/Biometrics_SIHR_ENG.pdf

²¹ibid

Palestinians, where over 2000 Palestinians were shot or killed in stampedes from May-July 2025 in efforts to collect aid²².

Conditional and coerced aid

In any case, aid is conditional on submitting biometric data. This violates fundamental rights to privacy and rights to receive humanitarian assistance free from coercion²³. Although framed as optional, the biometric scheme is the only option for women, children, elderly and wounded Palestinians to receive aid. Biometric data collection was also required to access the safe zones for aid collection. Beneficiaries are coerced into submitting biometric data, with a lack of informed consent or any real understanding of how their data will be used or stored.

Transparency

The GHF has not disclosed how its data is stored or any transparency in its list of donors²⁴, which casts greater risk of sensitive data being repurposed for military objectives. The GHF is funded by private American company Safe Reach Solutions, a US backed security logistics firm with extensive ties to military intelligence agencies²⁵. The Israeli military holds close alliances with the US military, and the GHF's humanitarian data has been used to train Israeli military facial recognition technology (ie Lavender weapons system), targeting Palestinians²⁶. The GHF's biometric technologies do not indicate prioritising humanitarian relief, instead acting as tools for surveillance. These risks introduced through collecting biometric data under pretexts of humanitarianism, call into question whether biometric technologies do more harm than good, particularly in the face of military funding²⁷.

5. Key Recommendations and Opportunities for Change

As has been shown throughout this Policy Brief, the integration of biometrics in humanitarian aid poses several harms to vulnerable populations. These harms make clear

²²Al Jazeera Staff, "US-Backed GHF Aid Mission in Gaza Ends: A Timeline of Violence," *Al Jazeera*, November 25, 2025, <https://www.aljazeera.com/news/2025/11/25/us-backed-ghf-aid-mission-in-gaza-ends-a-timeline-of-violence>

²³International Covenant for Civil and Political Rights, United Nations of Human Rights, 1996

²⁴Skyline International for Human Rights, "Biometrics for Food: A Dangerous Shift from Humanitarian Relief to Coercive Surveillance", May 15, 2025, https://www.skylineforhuman.org/admin/storage/files/shares/Biometrics_SIHR_ENG.pdf

²⁵ibid

²⁶'The Cost of Aid: When Humanitarian Data Collection Becomes a Method of Warfare'. 2025. *Opinio Juris*, November 6. <https://opiniojuris.org/2025/11/06/the-cost-of-aid-when-humanitarian-data-collection-becomes-a-method-of-warfare/>.

²⁷TRIAL International, "Human Rights, Legal Organizations Warn Privatized 'Humanitarian' Operators in Gaza of the Risk of Legal Liability for Complicity in Serious Violations of International Law," June 2025, <https://trialinternational.org/wp-content/uploads/2025/06/GHF-Letter-Public.pdf>

the importance of introducing and enforcing robust regulations and risk assessments that properly assess the safety of biometric systems and their immediate as well as longer term consequences. A 2017 Oxfam study revealed humanitarian biometrics failed to stop fraud, imposing more harm in extracting sensitive data, than relief benefits²⁸. While this may imply a call to remove biometric technologies from the humanitarian field entirely, this may be unrealistic at this point. Therefore the best recourse is to ensure that biometrics are managed responsibly to maximize their potential to support increasing humanitarian needs.

These following key recommendations seek to address the two largest harms identified in this brief: data protection risks, and accountability concerns.

5.1 DATA PROTECTION

RISK	RECOMMENDATION
Data Breach	1. More funding dedicated to ensure responsible development of biometric technologies. With increased private funding interests in developing biometrics, funders must also provide the resources for safe data storage and all sensitive data remain encrypted.
Experimental technologies deployed and exploiting vulnerable populations data	2. Establish an internationally recognised open source biometric template. This template can be an exemplary model of ethical data storage standards. Emerging biometric technologies need to be externally assessed by a board of specialists to approve their data protection guardrails adequately meet this standard. This will inform humanitarian organisations of the safe software they can use. Software which fails to meet ethical standards should be made illegal to use in the humanitarian sector.

²⁸The New Humanitarian, "Head to Head: Biometrics and Aid," July 17, 2019, <https://www.thenewhumanitarian.org/opinion/2019/07/17/head-head-biometrics-and-aid>

Function creep Long-term storage risks	3. Conduct regular cost versus risk analysis of data collection procedures. This analysis would help confirm humanitarian organisations are collecting biometric data only out of absolute necessity. These would include detailed justifications of why the biometrics are collected, for what purpose and establish how long it would be stored for. These analyses should be consistently reviewed to confirm that only strictly necessary biometrics are collected, and the data is erased after the purpose of its collection has been completed. This reduces the risk of long term data being used for other purposes.
--	---

5.2 ACCOUNTABILITY CONCERNS

1. Individuals must be given a choice. No data can be collected without **informed consent** of why the data is collected, and how it will be used. Users must have access to their own data and the right to retract their biometrics at any point.
2. We must be held **accountable to the individuals and communities** which have placed their trust in humanitarian aid.
3. **Hold humanitarians accountable** to their commitment to do no harm. Often criticisms are misdirected towards the technology itself rather than organisations practise and use of the technology.
4. Potential partners with humanitarian organisations must demonstrate a strong **commitment to cybersecurity**.

To conclude, this policy brief acknowledges the complexity of attempting to navigate using biometric data collection ethically. As biometric data collection gains momentum in the humanitarian context, it is important to mitigate its risks, while also harnessing the benefits it offers. We recognise that emerging technology has the potential to distribute aid more widely, and once the risks are recognised and properly avoided, could largely enhance humanitarian efforts to meet our ever increasing scale of need.

References

- Al Jazeera Staff. 2025. "US-Backed GHF Aid Mission in Gaza Ends: A Timeline of Violence." *Al Jazeera*, November 25, 2025.
<https://www.aljazeera.com/news/2025/11/25/us-backed-ghf-aid-mission-in-gaza-ends-a-timeline-of-violence>
- Faizan Farooque. 2025. "Palantir (PLTR) Lands \$1.3B Pentagon Win as AI Goes to War." *Yahoo Finance*, May 22.
<https://finance.yahoo.com/news/palantir-pltr-lands-1-3b-213719986.html>.
- Koops, Bert-Jaap. 2021. "The Concept of Function Creep." *Law, Innovation and Technology* 13, no. 1: 29-56.
- Madianou, Mirca. 2019. "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises." *Social Media + Society* 5 (3).
<https://doi.org/10.1177/2056305119863146>.
- Morley, Priya. 2024. "AI at the Border: Racialized Impacts and Implications." *Just Security*, June 28. <https://www.justsecurity.org/97172/ai-at-the-border/>.
- OHCHR. n.d. "International Covenant on Civil and Political Rights." Accessed April 20, 2026.
<https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- Pietropaoli, Irene, and Sara Razai. 2025. "Privatised Food Delivery in Gaza and Violations of International Humanitarian Law." *British Institute of International and Comparative Law*, July 24.
<https://www.biicl.org/blog/115/privatised-food-delivery-in-gaza-and-violations-of-international-humanitarian-law>.
- Rahman, Zara, Carly Nyst, and Paola Verhaert. 2018. "Biometrics in the Humanitarian Sector." *The Engine Room*, March 15, 2018.
<https://www.theengineroom.org/biometrics-in-the-humanitarian-sector/>
- Skyline International for Human Rights. 2025. "Biometrics for Food: A Dangerous Shift from Humanitarian Relief to Coercive Surveillance." May 15.
https://www.skylineforhuman.org/admin/storage/files/shares/Biometrics_SIHR_ENG.pdf.

The New Humanitarian. 2019. "Head to Head: Biometrics and Aid." July 17.
<https://www.thenewhumanitarian.org/opinion/2019/07/17/head-head-biometrics-and-aid>

.

TRIAL International. 2025. "Human Rights and Legal Organizations Warn Privatized 'Humanitarian' Operators in Gaza of the Risk of Legal Liability for Complicity in Serious Violations of International Law." June 23.
<https://trialinternational.org/latest-post/human-rights-legal-organizations-warn-privatized-humanitarian-operators-in-gaza-of-the-risk-of-legal-liability-for-complicity-in-serious-violations-of-international-law/>.

United Nations. n.d. "Crisis and Emergency Response." *Global Issues*. Accessed April 20, 2026. <https://www.un.org/en/global-issues/crisis-and-emergency-response>.

UN High Commissioner for Refugees. n.d. "Biometrics." *UNHCR Blogs*. Accessed April 20, 2026. <https://www.unhcr.org/blogs/?s=biometrics>.

U.S. Department of Health and Human Services. 2018. "The Belmont Report." *Office for Human Research Protections*. January 15.
<https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html>.

"Technocolonialism and Biometrics: Reinvigorating the Call to Decolonise Aid." n.d. *Forced Migration Review*. Accessed April 20, 2026.
<https://www.fmreview.org/digital-disruption/tsui-shaughnessy/>.

"The Cost of Aid: When Humanitarian Data Collection Becomes a Method of Warfare." 2025. *Opinio Juris*, November 6.
<https://opiniojuris.org/2025/11/06/the-cost-of-aid-when-humanitarian-data-collection-becomes-a-method-of-warfare/>