Selected Papers of #AoIR2025:
The 26th Annual Conference of the
Association of Internet Researchers
Niterói, Brazil / 15 – 18 Oct 2025

THE INFRASTRUCTURAL VIOLENCE OF THE USAID DATA CAPTURE

Mirca Madianou
Goldsmiths, University of London

On January 27th, 2025, hospital staff in Mae La refugee camp in Thailand received orders to shut down the hospital with immediate effect. Mae La is home to 37,700 Karen refugees, making it the largest refugee camp along the Thai-Myanmar border (The Border Consortium, 2024). By the end of January 28th, all patients had been discharged: those requiring emergency care were transferred to local hospitals in the nearby towns; others who needed treatment for non-urgent medical conditions were forced to return to their homes in the camp without any medication or clear plan. Other essential services such as water provision and waste disposal were also affected.

9,000 miles from Mae La, in Washington DC, over the same weekend, the offices of the US Agency for International Development (USAID) were raided by staff of the Department for Government Efficiency (DOGE) led by Elon Musk, the billionaire businessman. USAID, an independent US government department, had been the main donor to the NGOs providing humanitarian assistance in the refugee camps along the Thailand-Myanmar border. USAID was the first government department targeted by DOGE, an initiative of the Trump administration aiming to reduce federal spending. Thousands of USAID programmes across the world received ‘stop work’ orders while the USAID workforce was slashed from 10,000 to under 300 (Wired, 2025).

Back in Mae La, patients were told that in order to access medical care, they would need to pay not only for their medical costs in Thai hospitals, but also for transport and the camp passes which need to be issued to enter and exit the camp. Because of their status, refugees are not allowed to work, so raising a large amount of money is prohibitive. Naw Paw, who needed dialysis twice a week died two weeks after the hospital closed.

As Naw Paw and others were left to die, at the USAID offices in Washington a data grab was taking place. DOGE staff forced their way into secure rooms called ‘sensitive compartmented information facilities’ (Scifs). When USAID security officers tried to stop them as they didn’t have the necessary security clearances, Elon Musk demanded that

Suggested Citation (APA): Madianou, M. (2025, October). *The Infrastructural violence of the USAID data capture*. Paper presented at AoIR2025: The 26th Annual Conference of the Association of Internet Researchers. Niterói, Brazil: AoIR. Retrieved from http://spir.aoir.org

DOGE staff are given full access. The two USAID security officers who tried to prevent the data capture were suspended and then laid off.

The US government has been the main donor of aid to the over 103,000 Karen refugees who live in the 9 camps along the Myanmar-Thailand border (The Border Consortium, 2024). The 'zero tolerance to fraud' policy of the US government was interpreted by NGOs as an instruction to use biometric data to authenticate refugees in order to receive aid. According to the donors, biometric authentification reduces the possibility of refugees claiming aid twice. In 2018, the International Rescue Committee (IRC), which ran the camp hospital with USAID funds, started the biometric enrolment of all patients. Before the hospital closure at the end of January 2025, refugees were subjected to iris scans prior to medical treatment. Food assistance also requires biometric authentification through facial recognition. This logic of audit is not unique to Mae La but indicative of what happens across the humanitarian sector – the use of biometrics is ubiquitous.

Together with colleagues from Chiang Mai University we have been conducting research on the implications of digital identity systems in the refugee camps in Thailand (2024-2025). In total, we interviewed 65 Karen refugees and spoke with an additional 109 refugees through group discussions and participatory art sessions. Karen refugees have fled persecution and civil war in neighbouring Myanmar. Mae La, where our fieldwork took place, was established in 1984. Biometric technologies were first introduced in Mae La in 2015 when the United Nations High Commissioner for Refugees (UNHCR) conducted a biometric registration of the refugee population (UNHCR, 2015). Mae La exemplifies the digital identity roll out in refugee camps globally.

When he read the news about the USAID data capture, Saw Saw Guy, a Karen refugee who lives in Mae La asked a member of our research team: were our iris scans stolen by the DOGE officials?

It is unclear whether the data of Karen refugees were included in the USAID systems and whether non-government entities have access to the sensitive information. But the above example raises several questions about the implications humanitarianism's increasing dependence of data, digital innovation and AI.

In order to make sense of what connects the necropolitics in the refugee camp and the data grab in Washington DC, I develop the notion of 'infrastructural violence' (Madianou, 2025). To make sense of this term, we need to understand that humanitarian operations increasingly depend on digital technologies and forms of computation such as AI. With over 300 million people in need of humanitarian assistance, digital innovation and AI are championed as solutions to the challenges the aid sector faces. For example, biometric technologies were introduced to increase efficiencies and address allegations of low-level fraud. Biometric technologies such as facial recognition and iris scans, increasingly underpin a range of essential services from resettlement programmes to cash assistance and healthcare. Such systems are typically run by private companies. Crucially, we observe that humanitarian infrastructures (eg, food assistance systems) become interoperable with state or private sector systems (Madianou, 2024).

As with all infrastructures, humanitarian infrastructures remain largely invisible and depend on classifications that are inherently subjective (Bowker and Star, 1999). For instance, biometric systems depend on classifications regarding the physiological characteristics of the human body and reflect racist and gendered biases with colonial genealogies (Browne, 2015; Magnet, 2011; Buolamwini and Gebru, 2018). The invisibility of infrastructural classifications does not detract from their power. Quite the contrary, it places more urgency on recognizing infrastructures as sites of violence and political power. As digital infrastructures converge with humanitarian bureaucracies, they both inherit and amplify each other's limitations. This has profound implications for the character of humanitarianism and its sacrosanct principles of humanity, neutrality, independence and impartiality. For example, the principle of independence means that aid needs to be independent of state power or private interests. But when the infrastructure is privately owned and biometric data are shared with governments, can humanitarianism be independent? Similarly, the principle of humanity means that everyone is deserving of aid with no preconditions. Introducing a conditionality – relief is conditional on giving your biometric data – challenges the principle of humanity.

The decision by the US government to suspend USAID and freeze all aid programmes illustrates the infrastructuring of humanitarianism and the violence associated with it. A political decision in Washington DC, has immediate effects on life-or-death situations across the world. The flow of aid freezes immediately as the infrastructural tap is turned off. Underlying these processes are the colonial genealogies of humanitarianism as a form of 'soft power' serving the interests of donor countries (Donini, 2008). The infrastructuring of humanitarianism revitalizes and reworks these colonial legacies as 'technocolonialism' (Madianou, 2025).

Some harms resulting from the USAID freeze are less immediate. As digital and AI-based systems underpin all aspects of everyday life in the camp, their harms are generalised. As data infrastructures become more ubiquitous, the violence becomes more present and yet more diffused, almost like a form of ambient violence. I term this 'infrastuctural violence'. Infrastructural violence is a form of structural violence. It is an indirect form of violence which affects whole groups of people. But infrastructural violence is even more diffused and multiplied. As infrastructures transcend institutional boundaries and humanitarian systems become interoperable with those of private companies and nation-states, the opportunities for structural violence are multiplied. The shareability of data and the permanence of records can lead to function creep, which means that data collected for one reason may be used for entirely different purposes and by different actors than the original humanitarian organisations. Function creep amplifies the risks to individuals.

A less acknowledged dimension of the necropolitical situation unfolding in Mae La – and thousands of similar sites – concerns the risks resulting from the data grab in USAID. If sensitive data regarding some of the world's most marginalised people were accessed and shared, the risks are significant. If the biometric data of refugees, who have fled civil conflict and persecutions, fall in the wrong hands the consequences can be deleterious. The Myanmar government has a track record of obtaining the biometric records of its former citizens as happened with the data of the Rohingya refugees in Bangladesh (Human Rights Watch, 2021). As aid programmes come to an end due to the cuts in international assistance, the stewardship of databases containing the data of some of the world's most at-risk people becomes an urgent concern. While there is no concrete evidence about safeguarding breaches concerning the data of Karen refugees, the example of the USAID data capture reveals in stark terms the risks of the infrastructuring of humanitarianism and the vulnerabilities that this creates for some of the world's most marginalised people.

References

Bowker, G. and Star, S. L. (1999). *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: MIT Press.

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press.

Buolamwini J. & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification, *Proceedings of Machine Learning,* 81: 1–15.

Donini, A. (2008) 'Through a glass, darkly: Humanitarianism and Empire', in Gunewardena, N. and Schuller, M. (eds), *Capitalising on Catastrophe: Neoliberal Strategies in Disaster Reconstruction.* Lanham: Altamira Press.

Human Rights Watch (2021) UN shared Rohingya data without informed consent. https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

Madianou, M. (2025). *Technocolonialism: when technology for good is harmful*. Cambridge: Polity.

Magnet, S. A. (2011). *When biometrics fail: Gender race and the technology of identity*. Durham: Duke University Press.

The Border Consortium. (2024). Refugee Camp Population: December 2024. https://www.theborderconsortium.org/wp-content/uploads/2025/01/2024-12-December-map-tbc-unhcr.jpg

Schoemaker, E., Baslan, D., Pon, B., & Dell, N. (2021). Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. *Information Technology for Development*, 27(1), 13-36.

UNHCR (2015). ‘UNHCR’s new biometrics system helps verify 110,000 Myanmar refugees in Thailand’. https://www.unhcr.org/uk/news/stories/unhcrs-new-biometrics-system-helps-verify-110000-myanmar-refugees-thailand

Wired (2025) USAID Workforce Slashed from 10,000 to 300 as Elon Musk’s DOGE Decimates Agency. https://www.wired.com/story/doge-guts-usaid-workforce/