GEORGETOWN LAW
Center on Privacy & Technology

IM/MIGRANT WELL-BEING SCHOLAR COLLABORATIVE

Migrant Data Extractivism: Tech and Borders at the Limit of Rights

By Dr. Marianna Poyares in collaboration with the Georgetown Law Center on Privacy and Technology and the Im/migrant Well-Being Scholar Collaborative

INTRODUCTION

In a special issue article published in *International Migration* in July 2025, **Dr. Marianna Poyares**, Fritz Family Postdoctoral Associate (Lead) at the Georgetown Law Center on Privacy & Technology, presents the notion of "migrant data extractivism." As she argues in "**Migrant Data Extractivism: Tech and Borders at the Limit of Rights**," *migrant data extractivism* goes beyond mere user data collection, and sediments an ongoing shift within migration governance—from a system of rights, based on human dignity, to a system of sustained racialized dispossession, appropriation, and control. This shift raises critical questions as to the limits of human rights in the datafied world.

BACKGROUND

The concept of migrant data extractivism builds upon the foundation of frameworks such as migrant governmentality and of tech governance, which broadly refer to the set of systems, policies, and technologies governments use to control migration and human behavior. As Dr. Poyares explains, "the context of governance of (im)mobility then presents itself as a fertile ground for forced data mining… as certain products or technologies are imposed onto migrants." There is also a financial incentive for Big Tech agencies. Poyares focuses on two cases: the partnership between the International Rescue Committee (IRC) and OpenAI for providing chatbot-based educational services to refugees, and the collection and processing of migrant DNA by U.S. Immigration and Customs Enforcement (ICE). Stemming from drastically different contexts—humanitarian aid and immigration enforcement—these two cases reveal how migrant data extractivism has infiltrated migration governance. The research is backed by interviews with program coordinators (in the first case), government authorities (second case), and impacted individuals, as well as by legal research and large datasets' analysis of available documents and public records released through Freedom of Information Act (FOIA) requests.

CASE STUDIES

(1) Humanitarian chatbots as sites of data mining. The IRC's AprendIA program offers an AI-driven chatbot platform that delivers educational content to displaced populations. The chatbot operates through WhatsApp, which is linked to users' social media profiles. While filling an infrastructural vacuum, the partnership simultaneously gives OpenAI access to large populations whose interactions refine and optimize large language models. The scope of user data being collected through chatbot interactions or social media profiles, including personal and private information, remains unknown; the agency has no robust or clear privacy protection and data custody protocols.

(2) Department of Homeland Security (DHS) DNA collection. In 2020, following a change in language in the DNA Fingerprint Act, DHS began collecting DNA from immigrants under immigration enforcement custody. From 2020-2024, the agency stored over 1.5 million genetic profiles of migrants in the FBI's CODIS database indefinitely, labeled as criminal "offenders," absent any criminal suspicion. As it stands, migrant DNA collection requires no judicial authorization, no consent, and carries no statute of limitations. Migrants frequently believe cheek swabs are COVID

tests. The practice disproportionately targets racialized asylum-seekers, with consequences possibly extending to future generations through expanded genetic profiling.

KEY FINDINGS

INSUFFICIENCY OF INFORMED CONSENT PARADIGM

Migrant data extractivism exposes a fundamental weakness in the informed consent paradigm of privacy law. Forced migrants often face coercive conditions in which access to essential services, employment, or asylum processes is contingent on surrendering personal data. This asymmetry of power, combined with language barriers, opaque data practices, and limited legal recourse, undermines the idea that individuals can meaningfully understand or refuse data collection.

IMMIGRATION SURVEILLANCE INFRASTRUCTURE POSES PRIVACY CONCERNS FOR NON-CITIZENS AND CITIZENS

A vast web of technologies include ImmigrationOS (Palantir's case management system), geofencing apps (SmartLINK), social media spyware (Shadow Dragon), facial-recognition apps (Mobile Fortify), and many others. Since 2008, DHS has contracted with data brokers to access private information without going through the appropriate warrant requirements. This partnership alone has allowed the agency to access state driver's license databases for roughly 75% of U.S. licenses, independent of migration status.

NORMATIVE SHIFT FROM RIGHTS TO EXTRACTIVISM

As institutions and infrastructure are dismantled and replaced by contracted service provision, the racialized migrant is no longer recognized as a bearer of rights but treated primarily as a subject of data extraction.

PROFILING AND HARMS TO FUTURE GENERATIONS

The preemptive labeling of migrant DNA as "offenders" in the Combined DNA Index System (CODIS) in perpetuity, exemplifies how data systems encode profiling into their architecture. A genetic database composed predominantly of profiles from Latino and other racialized noncitizens extends surveillance and profiling into future generations.

RECOMMENDATIONS

Considering the potential civil and human rights violations (including those to the International Covenant on Civil and Political Rights and the Geneva Convention), in the context of migrant DNA collection by DHS, **we recommend that the program be discontinued**. This could be implemented via congressional action by removing authorization for DHS to collect DNA from migrants held without probable cause or on civil immigration charges. Congress could also **impose a statute of limitations on the migrant DNA collected**.

In the context of humanitarian agencies, **we suggest a complete inversion of the expertise workflow, prioritizing displaced communities first, then humanitarian expertise, and finally, technosystems**. Our recommendations include empowering local communities to independently assess systems for fairness and accountability, encouraging tech companies to invest in local humanitarian expertise, and developing an integrated governance approach that subordinates donations and procurement to human rights principles and safeguards.