

# **Regulating the Role of Private Technology Companies in the Collection and Storage of Migration and Refugee Data**

**Committee:** United Nations General Assembly (GA)

**Conference:** FISDMUN II

**Chair:** TBD

**Co-Chair:** TBD

## **Committee Overview**

The [United Nations General Assembly](#) is the primary body of the United Nations, where all member states have equal representation in addressing global issues. The General Assembly plays a key role in setting international norms and developing non-binding frameworks that guide state behavior.

This committee will focus on regulating the role of private technology companies in the collection and storage of migration and refugee data. Delegates will examine how emerging technologies are reshaping migration governance. The committee will explore how to balance efficiency and innovation with the protection of human rights and data privacy.

## **Introduction**

Private technology companies have grown to play a large role in managing migration and refugee data. This includes biometric identification, border control systems, and digital registration of refugees. The involvement of private technology companies has changed the way governments and organizations handle migrant and refugee populations by improving efficiency, but also raising serious concerns. While these technology platforms can streamline verification and management of data, they have also raised risks related to data privacy and surveillance.

Refugees and migrants are vulnerable because their data may be exploited without their knowledge or consent. The lack of clear standards for how private companies collect, store, and manage data has created major inconsistencies across countries. While some governments prioritize rapid technological innovation, others promote strict data protection, leading to contradictory policies worldwide.

Private companies aren't always held to the legal standards as governments raise concerns about potential sharing of data with third parties (law enforcement, foreign entities, etc), profit motives, and transparency. Without unified global regulation, there is an increased risk for human rights violations, discrimination, and confidentiality breaches. Mismanagement of data and a lack of regulation could endanger refugees, especially if sensitive information can be accessed by certain hostile groups. The United Nations is faced with the challenge to establish clear guidelines that regulate the role of private technology in migration data, while also respecting national sovereignty. Delegates must work to create a framework that protects vulnerable populations, accounts for efficiency, and promotes ethical use of technology in migration management.

## **Topic Background**

The role of private technology companies in managing migration and refugee data has expanded significantly in the 21st century causing it to rapidly grow as a critical global governance issue. International organizations have relied on private firms for digital identity platforms, data storage, and various systems to track and assist migrant and refugee populations. These technologies have proven to improve efficiency, however, the rapid expansion of technology has outpaced international regulations on the role of private technology companies.

One major concern is the lack of transparency in how private companies collect, store, and manage sensitive data. Refugees and migrants often blindly provide personal information without having comprehensive understanding on how it will be used or shared. This leads to potential risks such as data misuse, unauthorized access, and exploitation. Furthermore, these systems are created through private companies, posing a risk of incomplete data and errors which can affect important decisions about relocation or service access. These discrepancies can lead to unfair treatment and violations of human rights creating global issues.

Data security and privacy are also major concerns because large scale databases contain confidential information that may become the target of cyberattacks or be accessed by groups that could harm vulnerable populations. The expanding role of private companies managing sensitive information has raised accountability concerns as well. Different entities may not use the same ethical and legal frameworks, causing inconsistencies in data distribution across different regions. This leads to complications when factors such as cross-border data and profit motives are involved since regulations differ between countries.

It is essential for international communities to address these challenges especially as global displacement and digital systems continue to rapidly grow. The United Nations General Assembly must work to establish unified guidelines that regulate private sector involvement and promote international cooperation.

## **Past International Action**

International organizations have worked in recent years to address data protection in migration systems. In 2015, the United Nations High Commissioner for Refugees (UNHCR) introduced its Policy on the Protection of Personal Data of Persons of Concerns. This framework established guidelines for consent, data security and privacy which helped set a standard for protecting refugee data.

Shortly after, in 2018, the European Union implemented the General Data Protection Regulation (GDPR) which enforced a strict standard of rules on how personal data is collected, managed, and stored. This policy had significantly impacted how private companies handled migration data. It required private companies to hold utmost accountability and transparency when handling migration data and had heavy penalties for violations. The International Organization for Migration has also strengthened its Data Protection Principles in recent years and promoted ethical data collections. The United Nations has also

emphasized the importance of responsible data usage and encourages member states to adopt a more comprehensive framework to avoid possible risks in migrant and refugee data usage.

In recent years, governments and international organizations have increased regulation of private technology companies in refugee/migrant data systems. Ongoing discussions have focused on creating global frameworks for cross-border sharing and proper enforcement of regulations. Previous actions have improved awareness and laid the foundation for guidelines, but their impacts have been limited due to the rapid expansion of private technology entities' involvement and uneven implementation worldwide.

## Case Studies

The United States has implemented various protection measures at both state and federal levels such as the California Consumer Privacy Act (CCPA). These laws require private companies to have transparency with how sensitive data is collected and used. They do lack a comprehensive national framework, creating inconsistencies in how migrant and refugee data is managed.

China and South Korea have taken a stricter approach to data governance through the 2021 Personal Information Protection Law (PIPL). This law enforces strong government control over how private companies handle data. Countries have adopted different policies to regulate the role of private technology companies in data governance, with some prioritizing strict enforcement and others focusing on digital innovation. This has created uneven global standards in the protection of migrant and refugee data.

## Policy Recommendations

Delegates should consider the following approaches when drafting resolutions:

- **Ensuring Transparency and Consent:** Require clear communication on how data is used and obtain informed consent.
- **Enhancing Accountability:** Define the responsibilities of private technology companies in managing sensitive data.
- **Balancing Innovation and Protection:** Support technological advancement while safeguarding human rights.

## Questions to Consider

- To what extent are private technology companies involved in collecting, storing, and managing migration and refugee data worldwide?
- What are the possible implications of limiting or expanding digital systems of data management?
- How do data protection laws and enforcement differ across countries?
- What types of digital data require the most international regulation?
- What are the possible limitations of increased regulation of private technology companies in migrant and refugee data involvement?

## Questions a Resolution Might Address

- What steps should be taken to prevent misuse, data breaches, or exploitation of refugee and migrant data?
- How do countries reduce the gap in current regulatory frameworks on private technology companies' role in migrant and refugee data?
- What are the appropriate and ethical ways private companies should collect, store, and manage migration and refugee data?
- What policies can promote secure, fair, and transparent data use globally?
- How can countries worldwide effectively enforce regulatory policies on private companies' role in managing migrant and refugee data?

## Works Cited

“2015/United Nations High Commissioner for Refugees (UNHCR).” *U.S. Department of State*, 2017, 2009-2017.state.gov/f/evaluations/all/244465.htm. Accessed 2 Apr. 2026.

“A Million Refugees and Migrants Flee to Europe in 2015 | UNHCR.” *UNHCR*, 2015, [www.unhcr.org/news/press-releases/million-refugees-and-migrants-flee-europe-2015](http://www.unhcr.org/news/press-releases/million-refugees-and-migrants-flee-europe-2015).

CHELSEA.STRANGE, and CHELSEA.STRANGE. “The Impacts of Technology on Migration: From Decision Making to Integration - Tetra Tech International Development.” *Tetra Tech International Development - Improving Livelihoods and Empowering Local Communities through Integrated, Locally-Led Global Development*, 18 Dec. 2023, [intdev.tetratech.com.au/news/the-impacts-of-technology-on-migration-from-decision-making-to-integration/](http://intdev.tetratech.com.au/news/the-impacts-of-technology-on-migration-from-decision-making-to-integration/).

“Data Protection | UNHCR.” *UNHCR*, 2025, [www.unhcr.org/what-we-do/data-and-publications/data-and-statistics/data-protection](http://www.unhcr.org/what-we-do/data-and-publications/data-and-statistics/data-protection).

Kayondo, Barbara N. “IARAN.” *IARAN*, 8 Jan. 2025, [iaran.org/blog/data-privacy-refugees](http://iaran.org/blog/data-privacy-refugees).

Matlin, Stephen A., et al. “Digital Solutions for Migrant and Refugee Health: A Framework for Analysis and Action.” *The Lancet Regional Health - Europe*, vol. 50, 26 Dec. 2024, p.

101190, [www.sciencedirect.com/science/article/pii/S2666776224003594](http://www.sciencedirect.com/science/article/pii/S2666776224003594),  
<https://doi.org/10.1016/j.lanep.2024.101190>.

Poyares, Marianna. "Migrant Data Extractivism: Tech and Borders at the Limit of Rights."

*International Migration*, vol. 63, no. 4, 14 July 2025, <https://doi.org/10.1111/imig.70065>.

Spindler, William. "2015: The Year of Europe's Refugee Crisis." *UNHCR*, 8 Dec. 2015,  
[www.unhcr.org/news/stories/2015-year-europes-refugee-crisis](http://www.unhcr.org/news/stories/2015-year-europes-refugee-crisis).

State of California Department of Justice. "California Consumer Privacy Act (CCPA)." *State of California - Department of Justice - Office of the Attorney General*, 2024,  
[oag.ca.gov/privacy/ccpa](http://oag.ca.gov/privacy/ccpa).

*The Data of the Most Vulnerable People Is the Least Protected* | *Human Rights Watch*. 11 July  
2023, [www.hrw.org/news/2023/07/11/data-most-vulnerable-people-least-protected](http://www.hrw.org/news/2023/07/11/data-most-vulnerable-people-least-protected).

*The Role of Technology in Addressing the Global Migration Crisis*. 2018.

Wallace, Andrea. "Recent Immigrant Children: A Profile of New Arrivals to U.S. Schools."

*Open GLAM*, vol. 2, 19 Oct. 2020,

[www.netimpact.org/sites/default/files/documents/what-workers-want-2012-summary.pdf](http://www.netimpact.org/sites/default/files/documents/what-workers-want-2012-summary.pdf),  
<https://doi.org/10.21428/74d826b1.b1ae638e>.