Ukrainian Refugees

Forced Displacement Response Goes Fully Digital

Lauren Burke, Anastasia Strouboulis, Catherine Nzuki, and Erol Yayboke

As of mid-June, more than 7.3 million people had left Ukraine since Russia invaded in February. An additional 7.1 million people were internally displaced, representing one-third of the prewar Ukrainian population. Though almost 2.4 million people have crossed back into Ukraine, the speed and scale of forced displacement have been unprecedented compared to recent crises, putting tremendous strain on available services. This has prompted EU member states, the United Nations, aid organizations, private companies, civilian volunteers, and many other groups to expand operations and innovate service delivery.

The mobilization of these services is notable for the extent to which they are digitally driven. While most refugees have access to phones and the internet, Ukrainian refugees are not facing the additional challenges of rural network coverage and device and data plan affordability due to the robust digital infrastructure available throughout the region. At the start of 2022, Poland’s internet penetration rate stood at 87 percent of the total population (compared to, for example, 32 and 24 percent in Bangladesh and Uganda, respectively), and the number of social media users equaled 65 percent of the total Ukrainian population. These networks extend into the European Union, where, in 2021, 90 percent of households used broadband internet access and, in 2019, 73 percent of individuals used a mobile device to connect to the internet. As Ukrainian nationals and residents are forcibly displaced from one area to another, telecommunications infrastructure remains ubiquitous.

This connectivity has facilitated digitally based assistance and protection services. While digital tools have long supported in-person humanitarian assistance and protection services, digital solutions have been integrated into every step of the refugee assistance process for Ukrainians. Digital access has enabled refugees to connect and communicate with family, friends, and aid organizations, as well as remotely access real-time information, resources, and support using digital identification. Digitization has been important, in part, because most Ukrainians are staying in private residences in Poland and across Europe, rather than remaining in central locations. This crisis demonstrates that the expanding application of technology in refugee contexts can create new opportunities to empower displaced individuals and improve protection responses by host countries and aid providers.
However, these new tools also come with risks, including those associated with refugee protection. Though technological solutions have helped governments, nongovernmental organizations (NGOs), and humanitarian actors cope with the rapid influx of people, the need to scale up quickly has created gaps in protection, which run the risk of compromising refugees’ safety and privacy and exposing them to further protection risks. The Ukrainian context provides valuable lessons for practitioners navigating the deployment of digital technologies while addressing human rights risks at each stage of a refugee’s journey.

The Ukrainian context provides valuable lessons for practitioners navigating the deployment of digital technologies while addressing human rights risks at each stage of a refugee’s journey.

The Double Edge of Technology beyond the Border

Biometric technology has played a pivotal role in processing Ukrainians fleeing the conflict. As of 2021, over 13 million Ukrainians—more than one-third of the adult population—were using Diia. This smartphone app serves as a digital wallet for electronic versions of many official Ukrainian government documents—including passports and driver’s licenses—which hold the same legal status as their physical originals. Diia’s initial goal was to make it easier for individuals to access Ukrainian public services. In the context of the war, the platform has proven useful to refugees without physical copies of important
documents. However, some populations, such as the elderly, may lack the skills and resources necessary for access.

Overall, this arrangement is unusual in forced displacement situations; often, refugees are reluctant to share personal data with or rely on services from their country of origin due to the risk of state-sponsored persecution. Under international refugee law, asylum-seekers and refugees are not required to share their information with or contact authorities from their country of origin to establish identity. The circumstances of the Ukraine conflict, however, mean that Ukrainians can rely on digital identification provided by their home government without fear of surveillance and profiling by Ukrainian government authorities.

Robust digital infrastructure in European national governments has also increased the availability of data for humanitarian use relative to other crises. However, there are still gaps in data collection and validation, as well as in their relevance to government and humanitarian programs. For example, after refugees from Ukraine are initially registered at border crossings and Refugee Accommodation Centers, most continue into communities and countries beyond their initial point of departure from Ukraine. A byproduct of the freedom of movement is a lack of data—and data sharing—on where people are, if and where they are moving, whether they are separated from other family members, and perhaps most crucially, what their needs are. To address this issue, the European Union intends to establish a shared platform for registration under its 10-Point Plan.

With the increased use of biometric technology comes significant concerns about refugee data protection and privacy. Although the use of data collected from refugees is governed by the Charter of Fundamental Rights of the European Union and the European Union's General Data Protection Regulation (GDPR), there are challenges in ensuring transparency, consistency, and adherence to technical and normative standards for digital technologies, especially at international borders. For example, the European Council is considering a proposal to expand the European Union's biometric database of asylum-seekers to include the beneficiaries of the Temporary Protection Directive (TPD), which currently applies to Ukrainians. The regulations governing this database include specific privacy provisions, though they do make biometric data collection mandatory with a 10-year storage requirement for asylum-seekers.

Poland has argued that these privacy protections are “practically impossible” in the case of Ukrainian refugees due to limited human resources and storage capabilities. Ireland also raised concerns about interoperability between the personal data collected under the TPD and biometric information under this proposal. If not fully addressed, these early logistic and legal challenges to adding Ukrainians will renew concerns over surveillance, misuse, and coercion that human rights organizations have raised regarding the widening scope and purpose of this database. The GDPR, for example, allows the transfer of stored data given adequate safeguards or applicable derogations. However, removing certain measures, such as the one requiring explicit consent from individuals, could result in mass data transfers to third countries, including back to Ukraine. These risks are particularly concerning since Russian cyberattacks have targeted the Ukrainian border management ministry and aid organizations assisting Ukrainian refugees for unclear yet undoubtedly malign reasons.

Protecting the right to privacy is particularly important when asylum-seekers and refugees may not be aware of the rights and protections they are entitled to, and thus provide personal data without informed consent.

**Rights-Aware Utilization of Digital Tools to Support Refugees**

After displaced people have crossed an international border and escaped immediate physical danger, they confront new challenges. Governments, multilateral institutions, NGOs, and the private sector all play a role in supporting refugees, especially those who are decentralized, like most Ukrainian refugees. Here, too,
technology has reshaped the governance, service delivery, and operation of agencies to increase efficiency, accountability, and accessibility in support of Ukrainian refugees.

The Ukrainian government is using Diia to send financial assistance to those internally displaced by the Russian invasion. The United Nations High Commissioner for Refugees (UNHCR) is also expanding its distribution and protection services infrastructure by scaling up digital cash transfers. Ukrainians can register in person with their biometric data, producing a PIN that allows them to collect cash at ATMs. While fingerprint scans are being used in the Ukraine context, UNHCR employs a multimodal system of fingerprints, iris scans, and facial recognition in its other assistance programs. For example, UNHCR uses iris recognition technology to distribute cash assistance at Jordanian ATMs and supermarkets. As the war in Ukraine continues, UNHCR anticipates disbursing $76 million per month to refugees in Poland, Slovakia, and Moldova, mostly enabled by biometric technology.

Refugees entering EU member states can also access a wide range of reception and integration services online, including counseling, cultural orientation and language courses, education, employment, healthcare, and financial services. Free online platforms such as Ukraine School allow children and Ukrainian and international teachers to access educational materials and interact with one another, helping maintain consistency in education and lessening the burden on host communities.

The digitization of humanitarian assistance services also provides refugees with new channels to communicate with providers and report protection concerns. For example, UNHCR has an online dashboard for each refugee-receiving country—including those hosting Ukrainians—with information on getting international protection; accessing services; and reporting fraud, misconduct, and abuse. The Romanian and Moldovan governments collaborated with international aid providers and national civic organizations to establish an online information platform, called “Dopomohă”—meaning “help” in Ukrainian—for Ukrainian refugees to access assistance. Aid agencies are also leveraging technology-enabled data collection, analysis, and sharing to inform their operations. For example, the International Organization for Migration’s Displacement Tracking Matrix captures, processes, and disseminates internal displacement data, which, when coupled with a series of representative surveys, helps create a more holistic picture of Ukrainian internal displacement.

Meanwhile, the private sector has also mobilized its platforms and technologies to meet humanitarian needs. In some cases, businesses have offered free services that they facilitate via online platforms. Airbnb.org is funding short-term housing for up to 100,000 refugees fleeing Ukraine, while Uber is providing unlimited free trips from the Ukrainian border to destinations across Poland. There have also been innovative collaborations between the nonprofit and private sectors to enhance NGO capacity for carrying out humanitarian work. Tech To The Rescue, a Polish nonprofit that matches NGOs needing IT support with companies providing those services, launched the #TechForUkraine campaign shortly after the Russian invasion, with the dual aims of providing better humanitarian assistance and protecting Ukrainian IT firms from cyberattacks. So far, the campaign has recruited more than 450 IT firms—including big names like Amazon Cloud Services, Orange, Salesforce, Allegro, Netguru, and Divante—to provide pro bono support for NGOs. Among the campaign’s success stories is the uaSOS.org platform, which matches Ukrainian refugees with free accommodation offered by private individuals and institutions in Poland, the Czech Republic, Hungary, and Slovakia.

It is critical that this well-intentioned desire to help be matched with appropriate human rights due diligence to ensure adequate protection for vulnerable populations. Doing so will take time and deliberate action. Airbnb.org, for example, was flooded with donations and willing hosts in the wake of their pledge
and hoped to house people quickly. However, to avoid putting the refugees at the risk of exploitation, the company would not match families to hosts until they were adequately vetted, a process that requires adequate staffing (a challenge given the scale of the demand) and time. The same challenge is faced by initiatives like Ukraine Take Shelter, which also connected refugees with hosts willing to take them in. Though such platforms were lauded by many media outlets, they risk creating a false impression of safety. This is dangerous because many of them, unlike Airbnb.org, were not performing background checks on hosts, opting to "leave background checks to refugees" and including disclaimers on their websites to remind refugees that they are “ultimately responsible for their own safety.” As a result, human traffickers may exploit online platforms that link Ukrainian refugees to transportation and shelter, often by posting fake housing ads, posing as volunteer drivers, or identifying potential victims. Given that 90 percent of Ukrainian refugees are women and children, addressing these concerns is urgent. UNHCR has stressed the importance of thorough vetting systems to “register and screen organisations, companies, and individual volunteers offering support to refugees.” Verifying the identities of volunteers and running background checks on them, as the Israeli tech firm monday.com has been doing, is an essential first step that every technology company and nonprofit should take to reduce the likelihood of trafficking and fraud.

*It is critical that this well-intentioned desire to help be matched with appropriate human rights due diligence to ensure adequate protection for vulnerable populations. Doing so will take time and deliberate action.*

**Long-Term Solutions**

When refugees arrive at a destination where they can set up permanent or semipermanent residencies, they often turn their attention to handling legal processes and accessing long-term services. Within the European Union, digitization has changed countries' approaches to application management and processing, as well as to the interoperability of various institutions involved in migration and asylum application management. With the exception of Bulgaria and Slovenia, most EU member states use online systems at some stage of processing both residence permits and citizenship applications, with many of them using those systems to store, track, and process applications. In Latvia, Finland, and Ireland, refugees can communicate with a chatbot to help them navigate the asylum process, even before arriving in the country. In six EU member states (Germany, Finland, Hungary, Latvia, Lithuania, and the Netherlands), an artificial intelligence (AI) system reviews the initial application and triages refugee applicants, using language and knowledge identification, document-scanning technology, and facial recognition to detect fraud. Especially in the context of such a massive influx of refugees, these systems could allow for faster and more efficient processing of residence permit applications under the TPD and asylum applications for those who do not meet TPD requirements.

Of course, AI systems could also facilitate discrimination. People of color fleeing Ukraine already faced discrimination at border crossings, including being physically assaulted by border guards and being barred from entry. Romani people, even those with Ukrainian citizenship, were told in some cases that there was “no room” at emergency shelters and were forced into substandard, segregated facilities. AI systems can reinforce decisionmaking bias if they are not appropriately calibrated to consider race, language, age, gender, disability, and other factors among displaced populations. For example, the UK Home Office
was found to have used a computer algorithm to fast-track visa applications that built in more favorable results for many white applicants and more denials for people of color. Similarly, the predictive policing software considered for use by U.S. Immigration and Customs Enforcement has been criticized as “unfair and inefficient” because of its outdated and inaccurate data, which can entrench discriminatory decisionmaking. This is not a new issue; discrimination in visa processing predates the digital era. However, technology providers and governments face an uphill battle in developing automated systems that are capable of avoiding these preexisting biases; such systems should be viewed skeptically until they are able to prove otherwise.

Conclusion: Support and Protect

The Ukrainian displacement crisis offers several lessons on deploying technology to expand refugee access to services and protection, while maximizing respect for human rights. This includes ensuring adequate time, even in fast-moving refugee crises, to build in human rights due diligence and risk assessments for any systems being deployed. The appeal of digital systems is often their speed and efficiency; these benefits are lost if solutions fail to create sustainable protection for vulnerable populations. Human rights risk assessments should consider disproportionate impacts on the most vulnerable populations, including ethnic minorities, women, children, and the elderly.

The appeal of digital systems is often their speed and efficiency; these benefits are lost if solutions fail to create sustainable protection for vulnerable populations.

In addition, the diverse types of organizations participating in the immediate responses to the Ukrainian refugee influx highlight the need for better coordination and communication between stakeholders. A diversity of voices—including forcibly displaced populations—when conceptualizing, designing, developing, and deploying solutions is vital and can reduce the likelihood of negative human rights impacts. For example, had private-sector companies matching refugees with housing hosts spoken with aid workers and women, they might have taken steps to ensure better background checks or to take greater care in pairing more vulnerable refugees—such as solo female travelers—with verified households, avoiding safety issues and reducing opportunities for trafficking.

Finally, as technology plays an increasingly important role in refugee processing, assistance, and settlement, experts in privacy law need to be consulted to ensure that the refugees’ personal information and biometric data are being collected, stored, and shared in accordance with international human rights norms and data ethics frameworks. Consistent practices regarding informed consent, data privacy, data subjects’ rights, and information sharing are required among international organizations and national governments. Pursuing these protections must also include implementing robust cybersecurity standards and protocols, underscored by the recent cyberattack on the International Committee of the Red Cross, where hackers accessed the personal data of more than 515,000 people.

Although they offer great potential, there are fundamental challenges to the effective and human rights-protecting deployment of digital border technologies and digital systems for refugees. In anticipation of future mass displacement crises, stakeholders should adopt and strengthen human rights-based approaches to the development and use of digital technologies in border and human mobility management, underpinned by principles of transparency, equity, and protection.