Screening Technology Against Harms to Displaced Persons and Society at Large

A Proposal for Virtual Thematic Event 2: Privacy, Confidentiality, Data Protection, and Security

By: Bushra Ebadi and Jonathan Kent, Centre for International Governance Innovation

Context

Refugees, internally displaced people, and others forcibly displaced often do not possess passports or identity documents as a result of the persecution they are fleeing, the inadequacies of systems that fail to provide individuals with birth registrations and other forms of official identification. This presents a barrier for displaced persons, especially when aid and protection are tied to the ability of individuals to prove their identity through official documentation.

The increasing prominence of digital identification globally may present a viable alternative to more traditional forms of personal verification and has benefits in the context of forcibly displaced and highly mobile populations. It may help states gain a clearer understanding of who lives on their territory, assist the United Nations in efficiently distributing basic humanitarian aid, and allows refugees to access income remittances, financial transfers, online education, mobile phones, housing, and health care. It may be possible to file and assess asylum claims online; asylum claimants may be interviewed over the Internet and receive the outcome of the process via a block chain message key. The need for a more efficient, adaptable and accessible system for displaced persons increases the pressure to integrate digital identity into the lives of refugees, asylum seekers, and internally displaced persons.

Challenge

However, while emerging technologies and digital identity may enable solutions for displaced persons and the communities hosting them, they are not free from risks and harms. Many civil society organizations, such as Amnesty International, Access Now, etc. and academics are concerned about the unmitigated acceleration of emerging technologies and the proliferation of digital identity and biometric identifiers for vulnerable groups. Key challenges include: the lack of meaningful consent; the risk of racial, gender and other biases as a result of incomplete data sets; and the misuse or abuse of refugees' personal and biometric data, especially when this data is not protected and secured from entities that threaten or persecute displaced persons. Researchers also report that many asylum seekers are reluctant to provide biometric data because they fear this information will be used by law enforcement to deport or detain them.

Despite efforts by international organizations, such as UNHCR, Amnesty International, and Oxfam, the gap in protecting displaced persons and other marginalized populations from the harms and risks associated with emerging technologies and the digitization of identity continues to widen. The diverse set of actors involved or implicated by digital identity and the use of other emerging technologies necessitates multi-stakeholder solutions in order to advance greater accountability and transparency in the global refugee and IDP systems.

Proposed Solution

Following 1.5 years of consultations and research, the World Refugee Council set out a list of actionable recommendations to transform the global refugee and IDP systems in order to effectively realize greater accountability, responsibility sharing, predictable finance and political will. Following Action 45 of its report, *A Call to Action: Transforming the Global Refugee System*, the Council proposes the establishment of multi-stakeholder data protection and technology ethics board.

“The WRC supports the establishment of a data protection and technology ethics board in which companies designing applications for and with refugees and IDPs seek accreditation by disclosing their practices, committing to ethical handling of data, and mitigating the risks and potential harms of the products and services they are developing. This technology ethics board would involve a diversity of stakeholders and be developed in coordination with app providers, for example, Apple [Store] and Google Play.”

Ethics boards are not a new phenomenon. The fields of research and medical ethics emerged in order to protect humans (and sometimes animals) from unreasonable and foreseeable harms. The Nuremberg trials resulted in the Nuremberg Code in 1948, which stated that ‘the voluntary consent of the human subject is absolutely essential,” and thereby made it clear that subjects must give informed consent and that the benefits of research must outweigh the risks.

Until the last few decades, the ethics of technology was not a formalized discipline distinct from other branches of ethics. The term “technoethics” was coined in 1974 by philosopher Mario Bunge who argued that technologists must be held technically and morally responsible for the technologies they were designing and implementing.

Outside the fields of medicine and defense, the development of technology is not subject to an ethical review before it is released into markets, to be utilized by the general population. Existing regulations and legal frameworks are insufficient in protecting users and society as a whole from the risks and harms created or amplified by certain technologies. Populations who are already vulnerable face even greater risks and harms; refugees and other displaced populations who lack projections within existing legal frameworks often lack remedies that may be available to citizens. The ability for individuals to vote enables them to put pressure on their governments to enact legislation to protect citizens.

It is therefore recommended that technology ethics boards be established, with representation from civil society, refugees and other displaced populations where possible, ethicists, and technologists. There are two potential models that can be drawn on in order to design a technology ethics board that successfully mitigates harms and risks to displaced persons.

The first model would require any individual or organization that wishes to develop technology that could be used by displaced persons to pass a review by an independent multi-stakeholder ethics board. This board would provide certification or approval for the use of these technologies in the humanitarian, development and/or security contexts. However, this can be difficult to implement when displaced persons utilize technology unbeknownst to individuals working in these sectors. For example, it has been widely documented that asylum seekers and refugees utilize WhatsApp to navigate their journey and seek out information. In this case, the risks associated with the app would be best mitigated prior to its release to the public.

The second model for a technology ethics board would involve mandating technology companies and the platforms allowing individuals to purchase, download or use apps to ensure each app, device or technological innovation undergoes an ethical review. This review should ensure that the benefits of the technology outweigh the risks and that mechanisms are in place to protect users. Similar to the way in which medical ethics boards function, assessing the risks and benefits of new pharmaceuticals or medical treatments before they are made available to the general population, these technology ethics review boards would serve as a necessary check on the rampant proliferation and dissemination of technologies that could present harms to displaced persons, not to mention society as a whole.

Since, in many cases, it is difficult to predict exactly who will be displaced and which technologies they will be utilize or come into contact with, it is necessary to mitigate the risks and harms of technologies as a whole. While a certain subset of technologies (ex: biomedical, defence, etc.) undergo reviews, those that appear on online marketplaces for consumption by the general population often do not undergo a transparent and reliable ethical review.

This proposed solution only works if technology ethics is mainstreamed into education systems. Ethics courses or certificates should be mandatory for software and hardware engineers, developers, and others responsible for technological innovations. Just as structural engineers swear an oath to do no harm when developing infrastructure, computer engineers must also commit to do no harm in developing technologies. In order to effectively do so, they must understand the social and ethical implications of the technologies they are developing. To realize this change, education systems will need to be transformed so that they encourage and facilitate interdisciplinary learning, moving beyond rigid STEM models.

As states and regional bodies develop technology ethics codes, technology ethics boards will need to be developed in order to institutionalize and realize these ethics in the real world and move them beyond a set of principles. It is paramount that investments be made at all levels of governance in order to develop and implement systemic and sustainable reforms that champions the protection and agency of marginalized and vulnerable populations, including displaced persons.

Next Steps

In order to successfully develop technology ethics boards, it is paramount that all stakeholders be convened to design, develop and deploy a feasible and sustainable model that can be adapted to various contexts.

In the process of doing so, the following questions will need to be addressed:

- What are the impacts of emerging technologies on the modes of indigenous knowledge transmission?
- Do emerging technologies, as they are conceptualized today, prioritize certain forms of knowledge over others? If so, what is the implication of this on marginalized communities?
- How can technologies facilitate the agency of displaced persons?
- Are displaced persons able to opt out of digital identity schemes? What are the implications if they do choose to opt out? Are they able to meaningfully and consensually opt out (or opt in)?

Appendix

Figure 1: List of Relevant World Refugee Council Calls to Action

ACTION 1: The WRC calls for the establishment of a new independent partnership, the Global Action Network for the Forcibly Displaced, to promote changes to the global system for refugees and IDPs, including advocating for measures to strengthen accountability, governance, responsibility sharing and funding mechanisms.

ACTION 3: The WRC calls on religious, ethnic, business, academic, media, technology, municipal and other influential constituencies to put maximum pressure on the political leaders of their countries to take positive action to ensure protection, dignity, assistance, empowerment and solutions for refugees and displaced persons within their own countries and worldwide.

ACTION 41: The WRC urges online service providers to convene to explore ways of working together to make existing technologies accessible to refugees and IDPs at low cost, with a particular emphasis on ensuring excluded groups, such as women and girls, the elderly, people with disabilities, and people with diverse sexual orientations and gender identities, have access.

ACTION 42: The WRC urges online service providers to review and, if necessary, supplement existing platforms, so that technology representatives, refugees, IDPs and humanitarian aid workers can work together to share ideas on technological solutions to problems faced by refugees and IDPs.

ACTION 43: The WRC calls on researchers, policy makers and practitioners to create early warning systems using big data analytics and predictive techniques to forecast repression, incitements to violence and other forms of coercion that can lead to forcible displacement. Such technologies could also be deployed to anticipate the impact of large refugee movements on nearby cities and neighbouring countries, including their effects on vulnerable populations.

ACTION 44: The WRC calls on interested states and other stakeholders to spearhead a data privacy or data collection statement such as the Toronto Declaration that is based on fundamental human rights. This statement should be signed onto by host and donor countries along with technology companies.

ACTION 45: The WRC supports the establishment of a data protection and technology ethics board in which companies designing applications for and with refugees and IDPs seek accreditation by disclosing their practices, committing to ethical handling of data, and mitigating the risks and potential harms of the products and services they are developing. This technology ethics board would involve a diversity of stakeholders and be developed in coordination with app providers, for example, Apple and Google Play.