KALDOR CENTRE FOR INTERNATIONAL REFUGEE LAW
THE ALLENS HUB FOR TECHNOLOGY LAW AND INNOVATION
LAW BUILDING F8, UNSW SYDNEY NSW 2052 AUSTRALIA
T +61 (2) 9385 2227 | E caroline.compton@unsw.edu.au | CRICOS Provider Code 00098G

# Submission to the UNHCR's Global Virtual Summit on Digital Identity for Refugees 'Envisioning a digital identity ecosystem in support of the Global Compact on Refugees'

We are grateful to the United Nations High Commissioner for Refugees (UNHCR) for this opportunity to contribute to deliberations about the creation of a digital identity ecosystem for refugees in support of the Global Compact on Refugees. The implications of establishing digital identity mechanisms for refugees are potentially very significant, and we are glad that the discussion is taking place.

We are legal scholars working in the fields of development, digital technologies, displacement, international law and refugee law. Our submission highlights what we regard as key issues for consideration in the Global Virtual Summit and include both technical and social concerns, grouped as they relate to each of the Thematic Events.

## Thematic Event 1: The Global Compact on Refugees and the refugee digital identity ecosystem

- *The starting point for the conferral on or assumption of digital identity by refugees must be to enable and enhance refugees' agency; it cannot be premised on refugee passivity nor focused only on material needs.* In the context of the rollout of PRIMES now underway, UNHCR should continue to make use of its extensive know-how and lengthy experience in viewing refugee registration and identity verification as an opportunity for refugees to reassert, and experience anew, a sense of political agency and personal autonomy (both individually and collectively, in whatever group configurations make sense to the refugees in question). UNHCR's 1994 guide, *Registration: A Practical Guide for Field Staff*, rightly emphasises the importance of "promoting community responsibility and participation in all stages of the process", both for the task of registration and in the forging of "durable solutions for the population concerned" beyond registration. As UNHCR acknowledges in that context, refugee registration is a practice of polity construction; it entails the making of a political unit, comprising the registered refugee population at a given place and time. Moreover, it is potentially the first such process in which a refugee may participate after a traumatic fracturing of relations with their primary polity of affiliation – the home state they have fled. It is therefore important that any digital identity-making project in which UNHCR is involved is attuned to this important element and develops its dialogue and collaboration with refugee communities and sub-communities accordingly.

- *Stakeholders must be aware of the potential downsides of "economic inclusion" via digital identity and associated cash assistance, such as the risk of entrenching economic inequality and impoverishment through over-indebtedness.* The Call for Submissions emphasises that "digital identity [can] contribute to the delivery of multipurpose cash assistance and facilitate economic inclusion". That is a laudatory goal, but pursuit of that goal should pay careful

attention to the ambivalent effects that economic inclusion can potentially have in impoverished communities, such as associated risks of over-indebtedness.[1]

## Thematic Event 2: Privacy, confidentiality, data protection and security

- *It is inevitable that any digital data recording or processing system will involve errors, both in underlying data and analysis. Equitable and just dispute resolution mechanisms to permit refugee identification outcomes to be challenged will be extremely difficult to establish in many refugee processing settings, but the availability of such a mechanism is essential in all settings in which refugees' digital identities are being operationalised.* A number of factors complicate the challenge of enabling refugees to challenge the attribution or verification of their digital identity. There is often a power imbalance between government and agency workers, on the one hand, and the refugees and asylum seekers with whom they work, on the other. Moreover, frontline government and agency workers often tend to assume the "correctness" of biometric data. Careful attention must therefore be paid the way digital authorisation processes are perceived and understood by those who use them. Relevant workers should be cautioned against believing such systems are infallible and be made aware of the possibility and rate of errors. This is particularly important in settings where techniques for identification remain experimental (for example, identification from pattern-of-life data or the use of facial recognition software, discussed below). Further, it is vital that UNHCR develop dispute resolution mechanisms that acknowledge errors are possible (and indeed, inevitable) and provide a mechanism that provides a tangible way for refugees to dispute automated decisions and underlying data. A meaningful dispute resolution system can facilitate refugee and asylum seeker agency, as raised above.

- *UNHCR needs to be aware of relevant and emerging standards in designing PRIMES. These include, but are not limited to, ISO 8000, ISO/IEC 38505-1: 2017 and the IEEE suite of standards* (including new standards as they emerge, for example in the IEEE P7xxx series). Relevant UN instruments should also be referenced in the context of data governance.[2]

- *Related to the above, the choice of any given system entails different risks, vulnerabilities and biases, and makes possible different potential actions.* From a security standpoint, it is worth noting that refugee data can be particularly sensitive and there will be some states and other actors with the ability and incentive to exploit system vulnerabilities.

- *The selection of data to substantiate any digital identity must be tailored to the relevant identity and a minimum level of data retained for this purpose, to minimise the risk of data repurposing and/or unauthorised access or release. The temptation to develop expansive data sets and analytical tools to inform identity must be resisted in order to protect the inherent dignity of refugees and asylum seekers.* The ongoing advancement of pattern-of-life-type analysis increases the breadth of data that could contribute to the development of a digital identity including, for example, handwriting analysis and phone use patterns. Given the particular vulnerabilities of refugee populations, we would encourage extreme caution in the development of any expansively constructed digital identity. At a minimum, the assemblage

[1] Guerin, I., Morvant-Roux S., and Villarreal M. (eds), (2013) *Microfinance, Debt and Over-Indebtedness: Juggling with Money*. London: Taylor and Francis.

[2] OHCHR (2016) A Human Rights Approach to Data: Leaving No One Behind in the 2030 Development Agenda; UNDG (2017) Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection – Guidance Note.

and storing of data with a view to identification should be the subject of ongoing, informed consultation with refugee populations.

### Thematic Event 3: Emerging technologies and new developments

- *With reference to SDG indicator 16.9 and the goal of "build[ing] effective, accountable and inclusive institutions at all levels", the development of a refugee digital identity ecosystem must take account not only of how to collect, store and facilitate the responsible sharing of digital identity data, but also of when and how to enable the disposal and/or withholding of digital identities conferred on refugees.* A digital identity borne from displacement may be life-saving at some times and in some settings, but burdensome or intrusive at/in others. Once refugees have found a durable solution, consideration should be given to their entitlement to dispense with, or request the destruction ("deprovisioning") of, data comprising their digital identity. This may be desirable for a refugee to enjoy the kind of identity or anonymity that those who never sought asylum typically enjoy, or for other reasons personal to that refugee (e.g., to minimise the possibility of harm to family members and others remaining in the country of origin, or to mitigate the risk of exposure to domestic violence and/or lessen anxiety about that risk).

- *Biometric identification often seems to promise unprecedented precision and personalisation, but the ability of different biometric technologies to deliver on this promise varies significantly from technology to technology and population to population. Accordingly, any refugee identification system incorporating biometric data must provide for concurrent evaluation of that data's or system's reliability in particular subject populations.* For example, factors such as contact lens use, pupil dilation, corneal bleaching, scarring, inflammation and other pathologies – some of which may be especially prevalent among the impoverished or those who have otherwise not had access to regular healthcare – may negatively affect the error rate of iris recognition software.[3] Studies also show that commercial facial recognition software performs better on faces that are white and male.[4]

**Caroline Compton**, Research Associate
**Fleur Johns**, Professor and Associate Dean (Research)

**Data Science in Humanitarianism: Confronting Novel Law and Policy Challenges Project, UNSW Law**

**Lyria Bennett Moses**, Professor and Director
**Monika Zalnieriute**, Research Fellow

**The Allens Hub for Technology, Law and Innovation, UNSW Law**

**Guy S Goodwin-Gill**, Professor and Deputy Director
**Jane McAdam**, Professor and Director

**Kaldor Centre for International Refugee Law, UNSW Law**

[3] Trokielewicz M., Czajka A., Maciejewicz P. (2019) Iris Recognition in Cases of Eye Pathology. In: Nait-Ali A. (eds) *Biometrics under Biomedical Considerations*. Series in BioEngineering. Springer, Singapore.
[4] Buolamwini J., Gebru, T. (2018) Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research. 81: 77-91.