April 2019

Privacy International's contribution to Global Virtual Summit on digital identity

Privacy International welcomes the decision of the organisers of the Global Virtual Summit, the UNHCR and the Immigration, Refugees and Citizenship Canada (IRCC), to explore digital identity for refugees and asylum-seekers.

In this submission, Privacy International aims to highlight key areas which deserve further attention and should be addressed as part of the Global Virtual Summit.

I. Digital identity for refugees and asylum-seekers

Refugees are continuously exposed to threats and risks at various stages of their journeys, from the moment they flee their homes as they pass through transit, temporal places, i.e. refugee camps or detention centres, to their final destinations. Increasingly every interaction they have with a third-party be it humanitarian and development agencies to governments requires the processing of their personal data from enrolment/registration to identification and authentication. Previously, this data was primary collected directly by actors in the refugee ecosystem but it is now also being integrated with data from other sources, including from third-parties such as social media data, device-level data, and satellites[1] And there already sign that this trend is continuously expanding with ever-increasing invasive techniques being deployed at the border[2], and being integrated within refugee and asylum process.[3]

However, the adoption of such systems without the duty of care necessary from the onset means that existing challenges are intensified, and also new, different threats arise as those deploying digital identity solution are not prepared to mitigate the risks.[4] Any such adoption should start with a thorough evidence-based problem assessment to consider whether the lack of an ID is actually the root of the problem identified which can only be solved by the provision of one.

The challenges of identity, identification and ID are massive: human identities are complex, multifaceted and changing; the designs of identification systems is difficult to ensure inclusion, security and accuracy; yet the consequences of breaches or exclusion are large.[5] All these diverse challenges probably see their most challenging possible environment in the refugee context. The issues and challenges of the digital identity in the refugee context are massive:

---

[1] See: Privacy International, Communities at Risk: How Government are Using Tech To Target Migrants, 11 April 2019. Available at: https://privacyinternational.org/blog/2781/communities-risk-how-governments-are-using-tech-target-migrants; Laterno, M., Hiatt, K., Napolinato, A., Clericetti, G., and Penagos, M., Digital Identity in the Migration & Refugee Context: Italy Case Study, Data & Society, April 2019, pp 14. Available at: https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf

[2] Privacy International, Migration and Borders, Topic Page. Available at: https://privacyinternational.org/topics/migration-and-borders

[3] Privacy International, Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers, April 2019. Available at: https://privacyinternational.org/feature/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

[4] Privacy International, Development and Humanitarian Sector, Topic Page. Available at: https://privacyinternational.org/topics/development-and-humanitarian-sector

[5] Privacy International, Identity, Topic Page. Available at: https://privacyinternational.org/topics/identity

people who have lost papers and physical devices; consequences of identity and data misuse are grave.

II. Digital Identity: a legitimate aim?

Identities are extremely important; as SDG 16.9 states, a "legal identity" is a desirable goal. But a smokescreen has been thrown up surrounding this term; it is used to justify *any* identity system.[6]

In data protection terms[7], the 'legitimate interest' means that those looking to deploy digital identity solutions in a refugee context must clearly demonstrate that the processing is necessary and proportionate to the legitimate interest pursued and it does not override the rights of individuals. This requires the entity processing the data to clearly state the ground for processing, prior to the processing and any change must be compatible with the original purpose.

Ideas proposed by actors managing refugee processes to deploy their own digital identity system and/or make use others' can be as varied as registration, social and financial inclusion and keeping track of health services. It is within each of these purposes that the need for digital identity and the risks and obligations which come along with its deployment must be assessed and questioned rather than seeing digital identity as a single tool, or solution, to deliver each of those purposes.

The concerns observed in the refugee and asylum sector, as across many other fields, is that the data processed is then utilised for another purpose merely because it is available, and currently because of the nature of the sector there are little or no technical or legal barriers preventing what is called mission or function creep.

III. Harms of digital identities schemes

If humanitarian actors are to respect the principle of "do no harm" they must first understand the harms that can result from digital identities schemes. There are significant privacy risks arising from the deployment of technology in the context of humanitarian assistance.[8]

'*Visibility'*
A notion of the long-term benefits of digital ID often brings in an idea of "visibility", i.e. making people previously unknown to government authorities and the private sector known.[9] While the development community sees 'visibility' as an unquestioned good, the harms and dangers of being 'visible' must be recognised. The humanitarian sector must approach this with

[6] Privacy International, The Sustainable Development Goals, Identity, and Privacy: Does their implementation risk human rights?, 29 August 2018. Available at: https://privacyinternational.org/feature/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk
[7] Privacy International, The Keys to Data Protection: A guide for policy engagement on data protection, September 2018. Available at: https://privacyinternational.org/data-protection-guide
[8] International Committee of the Red Cross (ICRC) and Privacy International, The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era, October 2018. Available at: https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era
[9] Hanmer, L. and Daham, M., Identification for Development: Its Potential for Empowering Women and Girls, World Bank, 9 November 2015. Available at: https://blogs.worldbank.org/voices/identification-development-its-potential-empowering-women-and-girls; Pokharel, N. and Niroula, S., How a Legal Identity Leads to a Better Life, Open Society Foundations, Voices, 22 January 2015. Available at: https://www.opensocietyfoundations.org/voices/how-legal-identity-leads-better-life

more caution. The benefits of 'visibility' are contextual, and questions of visibility are at the centre of the notions of dignity and autonomy.[10]

Security
Complex IT systems are inherently vulnerable to intrusions or data breaches. There are numerous high-profile example of 'secure' IT systems being breached.[11] If some of the most well-resourced governments in the world are unable to protect their most sensitive data sources, it is reasonable to assume that resource-constrained host governments and humanitarian agencies will face significant challenges appropriately securing databases, while making them 'honey pots' for attackers. This will inevitably expose those enrolled in such databases to criminals and nation states, including actors from which they are seeking refuge.

Metadata
There are dangers brought to individuals and communities from the identification, tracking and profiling emerging from 'metadata'.[12] Digital identities, in their design and implementation, can bring serious risks in this regard. Depending on the design of the system, it may produce metadata about people's location(s) and the services they access. Decision may be being made on the basis of this information which raises risks not only for individuals, but also for populations, whose movements and activities can be tracked.

IV. Recommendations: Humanitarian Action in the Age of Digital ID

As demonstrated by Privacy International and its Network's work in this area[13], digital identity systems raises some key questions about legal, technical and ethical obligations in relations to upholding the rights of individuals and the protection of their autonomy and dignity as well as to the security and integrity of the data and the infrastructure being set-up.

These threats and risks are further heightened in a refugee and asylum context given some specific factors of this sector, which amongst others include:

- the vulnerable and challenging position of individuals seeking refuge and asylum and decisions made will impact their lives in the short- and long-term,
- the limited knowledge within the sector of data protection and security resulting in the lack of prioritisation of resources and skills-development to make informed decisions which respect the "do not harm principle", and
- the reliance on third-parties, in particular the private sector, which raises questions of control, transparency and accountability, as well as a threat of inappropriate influence from lobbying and the risk of facilitating corruption.

We recommend that the events and activities of the Global Virtual Summit address the following areas:

[10] Privacy International, Fintech: Privacy and Identity In the New Data-Intensive Financial Sector, December 2017. Available at: https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector
[1111] Perhaps most notoriously is the breach of the US Office of Personnel Management containing sensitive personal data of millions of US government employees. See: Koener, B., "Inside the Cyberattack That Shocked the US Government", Wired, 23 October 2016. Available at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/. For other examples from across the world, see: Privacy International, State of Privacy, 'Examples of data breaches'. Available at: https://privacyinternational.org/type-resource/state-privacy
[12] International Committee of the Red Cross (ICRC) and Privacy International, The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era, October 2018. Available at: https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era
[13] Privacy International, Identity, Topic Page. Available at: https://privacyinternational.org/topics/identity

- ***Taking a step back: why digital identity[14]***
    - What is the problem that the digital identity system is designed to solve; what evidence is there for the extent of the problem; and why would digital identity be a solution to that problem?
    - What alternative solutions are possible?
    - Is an identity solution that cuts across multiple actors or purposes desirable; and what risks emerge from this?
    - How are concerns related to intersectionality and gender to be addressed?
    - How to address donor and political pressures when the answer is that a digital identity system is not a desirable solution?

- ***Planning for the problem identified: Designing a system***
    - Does the design of the system meet the goals established in the purpose of the system, or does its design exceed those purposes to create additional privacy risks?
    - Has the technological design of the system provided for the maximum protection of the beneficiaries?
    - How will the digital identity system interact with the bureaucracies of host states?
    - Over what time-frame is the system designed to be used, and what is the data retention policy?

- ***Undertaking thorough assessments: preparing to fail well[15]***
    - What are the roles and motivations of state actors and private companies in the operation of the system, and is the data of refugees protected from further exploitation in the future?
        - Who holds the responsibility and so the obligations for the system (design, deployment, management, auditing, maintenance, etc.)?
        - How are new systems operating in relations to existing non-humanitarian identity systems, i.e. national ID systems?
    - What are the unintended consequences in the short-, mid- and long-term?
    - Does the entity deploying the system have the expertise, tools and resources to undertake a well-informed risk assessment and to mitigate the risks identified?
    - What minimum IT security measures should be implemented, and is there financial and technical support for such measures?
    - What will happen if any data in the database is breached by various actors?

- ***Understanding the lived experiences of refugees and asylum-seekers: human and ethical dimensions of digital identity[16]***
    - How do those who are affected by them experience the process?
    - What unintended impacts does the system have, for example in the impact upon survival strategies?
    - Who is excluded by the system, and what are the implications?

[14] Privacy International, Understanding Identity Systems Part 1: Why ID? Available at: https://privacyinternational.org/explainer/2669/understanding-identity-systems-part-1-why-id
[15] Privacy International, Understanding Identity Systems Part 3: The Risks of ID. Available at: https://privacyinternational.org/explainer/2672/understanding-identity-systems-part-3-risks-id
[16] Privacy International, Understanding Identity Systems Part 2: Discrimination and Identity. Available at: https://privacyinternational.org/explainer/2670/understanding-identity-systems-part-2-discrimination-and-identity