Centre for International Governance Innovation

WORLD REFUGEE COUNCIL

World Refugee Council Research Paper No. 12 — May 2019

Data Protection and Digital Agency for Refugees

Dragana Kaurin

Centre for International Governance Innovation

WORLD REFUGEE COUNCIL

World Refugee Council Research Paper No. 12 — May 2019

Data Protection and Digital Agency for Refugees

Dragana Kaurin

CIGI Masthead

Executive

President Rohinton P. Medhora
Deputy Director, International Intellectual Property Law and Innovation Bassem Awad
Chief Financial Officer and Director of Operations Shelley Boettger
Director of the Global Economy Program Robert Fay
Director of the International Law Research Program Oonagh Fitzgerald
Director of the Global Security & Politics Program Fen Osler Hampson
Director of Human Resources Laura Kacur
Deputy Director, International Environmental Law Silvia Maciunas
Deputy Director, International Economic Law Hugo Perezcano Díaz
Managing Director and General Counsel Aaron Shull
Director of Communications and Digital Media Spencer Tripp

Publications

Publisher Carol Bonnett
Senior Publications Editor Jennifer Goyder
Senior Publications Editor Nicole Langlois
Publications Editor Susan Bubak
Publications Editor Patricia Holmes
Publications Editor Lynn Schellenberg
Graphic Designer Brooklynn Schwartz
Graphic Designer Melodie Wakefield

For publications enquiries, please contact publications@cigionline.org.

Communications

For media enquiries, please contact communications@cigionline.org.
@cigionline

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

Research papers are policy documents commissioned by the World Refugee Council from world-renowned experts to help inform the work of the Council and its final recommendations. The measures and concepts in these documents do not necessarily reflect the views of the World Refugee Council.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Series

World Refugee Council research papers are policy documents commissioned by the Council from world-renowned experts to help inform the World Refugee Council and its final recommendations. The measures and concepts in these documents do not necessarily reflect the views of the World Refugee Council.

About the Author

Dragana Kaurin is a human rights researcher and ethnographer working at the intersection of technology, human rights and migration. Her past work includes researching the use of mobile phones by refugees in Europe and community tactics in filming police encounters in the United States. She is the founder and executive director of Localization Lab, a non-profit organization that works on technology adoption with local communities and provides user feedback. She is also a 2018-2019 research fellow at the Berkman Klein Center for Internet & Society at Harvard University.

Before starting Localization Lab in 2013, Dragana worked as a program officer at the Open Technology Institute, and as a data analyst at Ushahidi, a non-profit organization and mapping platform used for election monitoring and documenting violence using crowdsourced eyewitness reports. She holds bachelor's degrees in cultural anthropology and Arabic language from Ohio State University. Before entering the Human Rights Program at Columbia University, where she researched civic tech and refugee rights, she worked in crisis information management and C4D (communication for development) at the United Nations Office for the Coordination of Humanitarian Affairs and at the United Nations Children's Fund. She speaks French, Spanish, Arabic and Serbo-Croatian.

Acronyms and Abbreviations

CRC	Convention on the Rights of the Child
CTDs	Convention Travel Documents
DACA	Deferred Action for Childhood Arrivals
EURODAC	European Asylum Dactyloscopy
FTR	family tracing and reunification
FRONTEX	Frontières Extérieures/European Border and Coast Guard Agency
HIV/AIDS	human immunodeficiency virus/ acquired immune deficiency syndrome
ICCPR	International Covenant on Civil and Political Rights
ICRC	International Committee of the Red Cross
LGBTQIA+	lesbian, gay, bisexual, transgender, queer, intersex and ally
NGOs	non-governmental organizations
OCHA	UN Office for the Coordination of Humanitarian Affairs
RIP	Reception and Identification Procedure
UDHR	Universal Declaration of Human Rights
UNHCR	UN Refugee Agency/UN High Commissioner for Refugees
WFP	World Food Programme

Executive Summary

For the millions of refugees fleeing conflict and persecution every year, access to information about their rights and control over their personal data are crucial for their ability to assess risk and navigate the asylum process. While asylum seekers are required to provide significant amounts of personal information on their journey to safety, they are rarely fully informed of their data rights by UN agencies or local border control and law enforcement staff tasked with obtaining and processing their personal information. Despite recent improvements in data protection mechanisms in the European Union, refugees' informed consent for the collection and use of their personal data is rarely sought. Using examples drawn from interviews with refugees who have arrived in Europe since 2013, and an analysis of the impacts of the 2016 EU-Turkey deal on migration, this paper analyzes how the vast amount of data collected from refugees is gathered, stored and shared today, and considers the additional risks this collection process poses to an already vulnerable population navigating a perilous information-decision gap.

Methodology

Eleven interviews were conducted in English and Arabic with asylum seekers and refugees in Greece, Spain, Germany and Italy to capture their experiences of the asylum process in the European Union, and to record attitudes toward and beliefs about the collection of personal information and biometric data. The semi-structured interviews were conducted between August 2018 and January 2019, using snowball sampling. All interview subjects provided their consent for the use of the quotations that appear in this paper, and their names have been changed to protect their privacy.

The interviews were conducted to compare the subjects' lived experiences with the directives and policies of EU and humanitarian organizations tasked with collection of data. The interviews were supplemented with a review of relevant academic literature, legal documents and organizational policies regarding data collection and data protection. Current and former legal aid volunteers working with asylum seekers in Italy and Greece shared their insights on the systemic challenges of the EU asylum process and data collection, as did staff of the UN Refugee Agency (UNHCR) and the UN Office for the Coordination of Humanitarian Affairs (OCHA).

Introduction

The term "refugee crisis," as it was mediatized in 2015, when a record 1.3 million asylum applications were submitted in the European Union (European Statistical Office 2019), is one that is puzzling to refugees and asylum seekers alike. This crisis is framed in terms of the European Union's inability to control its borders and of the socio-economic impacts on host countries — instead of in terms of the crisis and trauma experienced by refugees fleeing the violence in Syria, Somalia and Afghanistan. For them, the crisis started long before they reached the EU border.

Refugees are expected to give vast amounts of personal information and biometric data while going through the asylum process in the European Union, to authorities, UN agencies and their implementing partners. They must provide personally identifying data, including sensitive information about surviving sexual violence, torture, war crimes or crimes against humanity. In order to make an informed decision about sharing sensitive data and information, refugees need to be able to assess the risks involved in doing so. They need to be able to trust the people and organizations requesting this data and to understand who it will be shared with and how it will be protected. Without this information, refugees navigate the system with uncertainty, making decisions that may ultimately cause them more harm.

Throughout this process, asylum seekers and refugees are stripped of their "digital agency," as they are forced to give up information and biometric data that they are no longer in sole possession of. Drawing on the definitions of agency from sociology, cognitive science and technology (Barker and Jane 2016; Jeannerod 2003; Kalantzis-Cope and Gherab-Martin 2010), digital agency can be defined as a sense of ownership and control over one's own electronic data, and the ability to independently create, access and make informed decisions about it.

Refugees fleeing war and persecution are in a vulnerable position because their country of origin does not afford them protections; indeed, often it is their own governments that are persecuting them. Once they cross the border into another country, they have fewer rights as non-citizens in their host country, which leaves them vulnerable to abuse. While the UNHCR and many non-governmental organizations (NGOs) have a mandate to protect refugees, the laws related to their protection are rarely enforced. Refugees also cannot rely on protection from law enforcement and legal mechanisms in host countries that protect citizens, because many law enforcement agencies are specifically tasked with finding, detaining or deporting them (Purkey 2013). This also means that, without equal access to mechanisms that enforce data protection laws, refugees are particularly vulnerable to violations of their rights.

A global struggle to achieve data protection laws and safeguards for consumers has emerged in response to the rapid growth in information technology and data privacy concerns. Refugees' inability to access legal mechanisms of protection results in a gap between their data protection and privacy rights and those of citizens of the host country they reside in. Expansive data collection in the humanitarian sector is concerning, especially with regard to security, proportionality and sharing of data, and is in need of more sophisticated safeguards to protect vulnerable individuals who are treated as mere data subjects.

Surveillance programs, such as the European Border Surveillance System, have been found to acquire refugees' data without their consent and knowledge (Kift 2016). This activity further hinders refugees' ability to control their own information. The very devices refugees use to navigate, translate, send and receive money, connect with family, and even employ as a makeshift flashlight when necessary (Kaurin 2016) are used by governments and private sector actors as powerful instruments of surveillance (Taylor and Graham-Harrison 2016). Social media platforms have been scrutinized for collecting and harvesting information, especially amid reports of spying on asylum seekers (Meaker 2018). Even when refugees are aware of the possibility of government surveillance, they rely on social media as an important source of information and connectivity. It is also perceived as a reliable way for humanitarians and legal aid volunteers to get in touch with refugees on the move, since their addresses, conditions and phone numbers often change (Bellanova, Jumbert and Gellert 2016).

Requiring biometric data from asylum seekers, as has become common among governments, UN agencies and NGOs, presents both challenges and opportunities. UN agencies, such as the World Food Programme (WFP), argue that being able to confirm an individual's identity at any time or location through an iris scan presents many opportunities for refugees (Rahman 2018). Another justification behind the use of biometrics in the humanitarian sector is that using this type of authentication may reduce instances of fraud, although there is no research available that proves this claim. Furthermore, the lack of transparency on why this data is collected, the lack of digital security and the sharing of data with host countries have been criticized by a number of NGOs such as Caribou Digital and Privacy International.

The following paper identifies the information gap and lack of digital agency faced by asylum seekers during the asylum process, and it analyzes the lack of transparency and accountability around both how technologies operate and how data is subsequently collected, used and protected. It provides an overview of the data protection policies and practices of entities collecting personal and biometric data from asylum seekers entering the European Union. Interviews with refugees and asylum seekers about how they navigate the asylum process with the information they are given or are able to find on their own will be used to better understand the impact of these policies on the refugee community. Finally, the paper will provide recommendations for the European Asylum Dactyloscopy (EURODAC), UN agencies and NGOs for restoring the digital agency of asylum seekers and refugees and for seeking informed consent from data subjects.

What Data Is Collected from Refugees?

Asylum seekers are expected to give vast amounts of personal information and biometric data throughout the many stages of the asylum process, the information required varying slightly depending on the EU country where they claimed asylum. Upon arrival in Europe, asylum seekers are subject to screening, photographing and fingerprinting[1] for those 14 and over,[2] done by local law enforcement and FRONTEX[3] (Box 1). Anyone who enters the European Union without a visa is considered an "irregular migrant" and their fingerprints are taken immediately upon entry, sometimes by force (EC 2016/0132(COD)). Fingerprinting is done to enforce the Dublin Regulation.[4] If they do not have any documents that prove their nationality, they are asked a series of questions about language, geography, history and customs in their country.[5] In Denmark, under Danish law, immigration officials can request social media passwords from asylum seekers to verify their identity and nationality (Meaker 2018).

Asylum seekers go through the Reception and Identification Procedure (RIP), an eligibility assessment, full registration and an asylum interview, in order to be considered for refugee status. UN agencies involved in the asylum process also collect, share and store personal information and biometric data for refugee registration and aid distribution.[6] This is the time when an individual claims their intent to apply for asylum and the determination of vulnerability status is done (Asylum Information Database, n.d.). Unaccompanied minors, handicapped persons, elderly people, and pregnant and nursing women are considered vulnerable and prioritized in the asylum process, as are victims of torture and sexual violence (Greek Law 4375/2016: 28 art. 9; see Greece 2016) (Box 2).

Box 1: Data Required at the Border

→ Name

→ Age

→ Place and date of birth

→ Fingerprints

→ Photograph

→ Nationality

Data sources: RefuComm (2018); www.refugee.info.

When it comes to cross-cutting issues surrounding applicants in the asylum process — such as gender-based violence, gender and sexual minorities (LGBTQIA+),[7] physical and mental disabilities, HIV/AIDS[8] and age-related issues (for example, vulnerabilities experienced by unaccompanied minors or the elderly) — asylum services are supposed to take special care to create safe conditions for sharing information. This isn't always the case for people from these marginalized groups; if they do not have an opportunity to do their asylum interview alone, or if they do not know who will see this information, they are not able to make informed decisions when they share such sensitive information.

One individual explained how, not knowing what would be done with this information, he had to explain the sensitivity of these issues to the Greek official asking him questions during RIP. Throughout the author's interview with this individual, in particular, it became evident that for many it is not possible to give informed consent, because data subjects do not understand what asylum status entitles an individual to, what the conditions are for granting asylum and even, on a more basic level, who is interviewing them and what they will do with the information that is collected.

[1] In Italy, this process is called the *fotosegnalamento*.

[2] There is currently a EURODAC legislation in the European Parliament awaiting vote that would lower the age of fingerprinting and photographing from 14 to six.

[3] FRONTEX — known variously as Frontières Extérieures and the European Border and Coast Guard Agency — is an EU agency tasked with border control of the European Schengen Area, in coordination with the border and coast guards of Schengen Area member states.

[4] The Dublin Regulation is an EU law that determines which EU member state is responsible for the examination of an application for asylum, and that prevents an asylum seeker from submitting multiple applications in the European Union.

[5] See www.refugee.info.

[6] Ibid.

[7] Although the UNHCR states their commitment to asylum seekers and refugees who identify as LGBTQIA+ (lesbian, gay, bisexual, transgender, queer, intersex and ally), the asylum process still poses risks and obstacles for them, including the various registration and family tracing and reunification (FTR) forms produced by the UNHCR. When giving information about themselves to the asylum official, stating one's gender is a binary option of male or female on all forms, making the process more complicated for transgender and non-binary asylum seekers. The UNHCR forms available in English also use "sex" and "gender" interchangeably, despite these terms' different meanings — biological sex and gender identification, respectively.

[8] Human immunodeficiency virus/acquired immune deficiency syndrome.

Box 2: Data Required at the RIP Stage

→ Name

→ Age

→ Gender

→ Verification of documents and determination of nationality. If the person doesn't have any identification, they will be asked a series of questions about their country for verification, for example:

- language
- cultural customs
- national currency
- flag

→ A medical screening to check the individual's health condition and to try verifying their age

→ Questions regarding one's claim to asylum

→ Determination of vulnerability status. Those who are given vulnerability status are:

- women who are pregnant or nursing;
- single parents of children under 18;
- unaccompanied minors;
- survivors of rape, torture, sex trafficking, female genital mutilation or other physical or psychological violence; and
- those who are over 65, have a serious illness or disability, or suffer from post-traumatic stress disorder.

Data source: RefuComm (2018).

Note: RIP = Reception and Identification Procedure.

> *I live with two personalities inside me, I have two faces. One person who is gay — who is comfortable with [himself], accepts his personality and his sexual orientation, but doesn't talk about it with others. Especially not with family. And the other — the straight, or "the normal person" — someone who would marry a woman, and walks like there is nothing wrong. It's very hard to explain it to a person asking these questions in the interview because I was very nervous to speak, and a little uncomfortable to tell them anything. They said "Hey, this is serious!" so finally I said "Okay, I'm gay. I'm from Syria, and I can't talk about that publicly. I left Syria because of war, but also I have this other problem."*
>
> *It's hard for many people to [get refugee status] here if they don't want to say sensitive things like this, or they can't say it because other family members are sitting next to you. Or to say that it can be dangerous if they return to Turkey, or what other country they came through. So, they must say these things, but they don't have the right opportunity to say it, or they don't know what they need to say; some of them experienced a lot of war, and have [mental health issues] and need to be helped through the process.*
>
> —Mohamed, 24, Syria

The full registration interview is done by the Greek Asylum Service in Greece, and by the Territorial Commission in Italy, who may request more information to ensure adequate protection and assess vulnerability[9] (Box 3). The process is similar when the UNHCR runs registration, although it is not any more informative for the asylum seekers. The final question in the general form used to register individual asylum claims is the following[10]:

> In seeking a durable solution for you in the future, do you authorise UNHCR to share the information contained on this form with other agencies and/or governments as may be required?
>
> □ Yes □ No

[9] See www.refugee.info.

[10] See Annex 6(c) of the UNHCR's *Handbook for Registration* (UNHCR 2003, 262).

Box 3: Data Required at Full Registration

- → Name and address
- → Size of family
- → Age of family members
- → Date and place of birth
- → Sex
- → Language spoken
- → Whether the applicant is applying for asylum, family reunification or relocation
- → Existing national identity number
- → Marital status
- → Special needs (e.g., certain health conditions and disabilities)
- → Level of education
- → Occupational skills
- → Ethnic origins
- → Religion
- → Languages spoken
- → Date of arrival
- → Information about medical or health status
- → Personal data about non-accompanying family members
- → Reason for flight
- → Intentions of return
- → Place and date of return
- → Family property
- → Means of arrival
- → Place of local integration
- → Resettlement opportunity and place and date of resettlement

Data sources: www.refugee.info; Bohlin (2008).

For refugees, this is a critical moment, and to answer this binary question correctly, they need to have understood the exact conditions for and the risks associated with sharing information.

For those who arrived after March 20, 2016, when the EU-Turkey deal[11] came into effect, the asylum process has become longer and more difficult. Currently, only vulnerable cases are transferred from the EU "hotspot" islands[12] to the mainland after registration, and the rest go through an extra interview to be eligible for the asylum appointment In Greece, if they come from one of the countries with high recognition rates of asylum,[13] they will undergo an admissibility interview, to examine whether it is a safe country for them to return to (see Box 4). Those who are not from these countries undergo an eligibility interview, where authorities will ask what compelled them to leave their country of origin. Authorities will then decide if they are eligible for the asylum interview in Greece. In Italy, this is done through a form called *Folio Senzone* that asylum seekers fill out.

The asylum interview is traditionally done by states, with the International Organization for Migration and the UNHCR taking on a supporting role where necessary. In both Italy and Greece, if the individual is granted an asylum appointment at this stage, it is usually scheduled for months, or even years, later, due to limited resources. During

[11] On March 18, 2016, the European Union and Turkey adopted the EU-Turkey Statement, a non-binding document more commonly known as the EU-Turkey deal, designed with the purpose of managing the migration flow into the European Union and, some say, of deterring refugees from coming to Europe. At the core of the deal is a commitment from Turkey to manage sea crossings into Greece, a deal for the European Union to give €3 billion to Turkey in aid, and a policy of swapping asylum seekers: "For every Syrian refugee being returned to Turkey from the Greek islands, another Syrian will be resettled to the EU taking into account the UN Vulnerability Criteria" (Council of the European Union 2016).

[12] "Hotspot" islands are the 10 Greek and Italian islands designated by the European Union to act as a second border, to curb the arrival of irregular migrants from Turkey and Libya.

[13] Admissibility interviews are given to asylum seekers from countries that have high recognition rates of asylum as well as stateless people. The European Union determines these countries; they are usually places affected by conflict, such as Syria, Iraq, Afghanistan, Yemen and South Sudan.

Box 4: Admissibility Interview Questions *(for some asylum seekers coming from Turkey to Greece)*

Admissibility interviews are for asylum seekers:

→ from a country with a high recognition rate of asylum (Syria, Iraq, Iran, Afghanistan);

→ classed as vulnerable; or

→ eligible for family reunification.

During this interview, authorities decide whether the asylum claim should be examined in Greece or the applicant will be deported back to Turkey. Asylum seekers are asked:

→ What happened during their stay in Turkey?

→ How long did they stay in Turkey?

→ Is Turkey a safe country for them to return to?

→ What might happen to them if they return to Turkey?

Data sources: RefuComm (2018); www.refugee.info.

this time, asylum seekers have limited movement on the hotspot islands. When the appointment time arrives, individuals are fingerprinted again and asked for some of the same information they had to give during RIP and the full registration. The focus of this interview, however, is to ask why they left their country of origin, and what would happen to them if they were to return. The responses will ultimately be used by authorities to decide whether to grant someone asylum[14] (Box 5).

How Asylum Seekers Experience the Process

Language is one of the biggest challenges for asylum seekers throughout this process. At the initial asylum registration interview, paperwork is filled out in local languages, using very different script from the languages most refugees speak. For example, Arabic, Dari and Kurdish each have their own alphabet and need to be transliterated into scripts of local European languages. Transliteration can result in many spellings of one name, which can make it more difficult to locate the data or case files of a particular asylum seeker.

Interpretation is often either lacking (due to too few interpreters) or inaccurate, even though domestic law states that asylum seekers should be informed about the registration procedure and their rights and obligations in a language that they understand (Greek Law 4375/2016; see Greece (2016), 40). This shortfall leads to mistakes, such as minors being registered as adults, the wrong nationality being recorded or other basic information being recorded inaccurately, such as the place of birth being registered instead of the name of the individual. Once the data is registered in the system, it is often very difficult for the individual moving through the asylum process to correct it.

One refugee from Somalia explained how the lack of adequate translators can exacerbate the situation for refugees. He noted that in Lampedusa, either translators were unavailable or the agency doing the processing failed to notify asylum seekers and refugees of the right to speak with a translator, or to speak with an interviewer of the same sex, where necessary.

> *When we arrived in Lampedusa, they [took] fingerprints from everyone, and they said it was because we broke the law by coming in a boat. They will not tell you anything, what you think doesn't matter — even if you say you don't want to give fingerprints, they'll take it anyway. Before we reached Lampedusa, people told me that I will be detained when we arrive because I was 15 years old then, and travelling to Europe alone. So, when I arrived, I told them I was 19, and I didn't have any documents with me that*

[14] See www.refugee.info.

said how old I was. Sometimes you have to tell a small lie to keep moving forward.

My interview took three hours: "Why did you leave your country? How did you arrive? Why don't you go back home?" It's not like I trust them, but it's your duty to say the truth, even the pretty private questions. You must tell them about all the difficulties at home, and what will happen to you if you go back. There is no information in our language, there is nothing available to say what will happen next, what they will do with the information — it's up to you to find it online. I used to translate for people while I was there, with an organization called Cittadini del Mondo. It is especially hard for Muslim women, because you get shamed for [sexual] violence, so it's difficult to talk about it, and many women don't say anything even when I explain it's important. There is no female translator there, and they can't give the details, even though the police keep asking.

—Samir, 19, Somalia

Box 5: Asylum Interview

Applicants are asked:

- why they left their country of origin;
- what would happen to them if they were to go back (they will need to share specific details such as the dates and times of the events that forced them to leave their country of origin);
- the date, time and places where these events happened;
- what other people were involved in these events;
- how they arrived in Europe;
- if they were part of any armed group or military; and
- details about their health, education and career.

As well, applicants may have their fingerprints taken again.

If the claim is accepted, the asylum seeker will receive one of two kinds of protection:

- Refugee status (full asylum) or
- Subsidiary protection (partial asylum).

Data sources: www.refugee.info; Bohlin (2008).

Biometric Data

Law enforcement and border control agencies such as EURODAC are not the only ones collecting biometric data from asylum seekers and refugees. UN aid agencies and NGOs also use biometrics in the form of fingerprints, iris scans and facial recognition technology for registration of beneficiaries and for aid distribution. Biometrics can be defined as any kind of "automatically measurable, robust and distinctive physical characteristic or trait that can be used to identify an individual or verify the claimed identity of an individual" (Woodward et al. 2003, cited in Rahman 2018, 4). Biometrics are commonly classified into biometrics for verification (one-to-one authentication), and biometrics for identification (one-to-many authentication), the latter requiring a larger amount of data and also tending to produce more false matches in the process (Rahman 2018, 6).

The EURODAC

The main purpose of the EURODAC database is to effectively enforce the Dublin Regulation, that is, to prevent multiple asylum applications and unauthorized entry. Fingerprints taken from asylum applicants are submitted digitally to a central unit at the European Commission and automatically checked against other prints in the database. This process enables authorities to determine whether asylum seekers have either already applied for asylum or illegally transited through another EU member state (European Commission 2016). Several refugees interviewed for this paper reported being deported back to Italy or Greece from elsewhere in the European Union after law enforcement representatives took their fingerprints and determined where they had applied for asylum.

Article 29 of EURODAC regulation (Regulation (EU) No. 603/2013)[15] gives explicit rights to data subjects: the right to access data relating to them, to request that inaccurate data be corrected and to have unlawfully processed data erased. The regulations, however, do not go into detail or give examples of what constitutes "unlawfully processed data." It also gives subjects the right to request information on how to exercise these rights, as well as the right to bring action or complaints against "competent authorities" of the state that recorded and stored an individual's information in a database. While these regulations and protections serve as mechanisms intended to build digital agency and to give asylum seekers some control over their own data to mitigate risks, none of the asylum seekers and refugees interviewed for this paper said they were aware they had these rights and options.

In 2016, a regulation on EURODAC was passed in the European Parliament that requires fingerprinting of every "irregular migrant" and condones detention and use of force in obtaining fingerprints, if the individual refuses to comply (European Commission 2016, 14, 25, 35). Another EURODAC regulation was passed in 2018, although it is not yet enforced, lowering the age of those fingerprinted from 14 to six, and allowing "some use of coercion" on minors in order to obtain their fingerprints. The justification for extending the scope of EURODAC is to prevent cases of child trafficking, although there is no evidence that collection of biometrics prevents trafficking, or clarity on how specifically biometrics will act as a child protection mechanism in the European Union (European Parliament 2018).

UN Agencies and NGOs

Some UN agencies, including the WFP and the UNHCR, use biometrics for identification purposes, specifically, iris scans and fingerprints to register beneficiaries and distribute assistance. One of the most frequently cited justifications for using biometrics in the humanitarian sector is that they reduce fraud and duplication, ensuring aid does not go to the wrong person or that one person does not get more than what was allocated for them. On their journey to safety, refugees often lose their travel documents and identification, or do not have an opportunity to take them at all. This poses many challenges for access to aid and services, which humanitarian organizations and other stakeholders claim can be addressed with the use of biometrics as identification (Rahman 2018).

If the UNHCR decides to use biometric identifiers[16] in Convention Travel Documents (CTDs), which are travel documents the organization issues to refugees, biometrics may also have the potential to aid refugees in freedom of movement. Due to perceived security threats, law enforcement and border control agencies often discredit the authenticity of CTDs and refugee registration documents. Many states have adopted biometric identifiers on their passports; applying them to CTDs may help in preserving refugees' freedom of movement because they work as a second authentication for border control. Biometric identifiers on the CTDs might also prevent unnecessary detention when refugees get stopped by law enforcement (Farraj 2010, 908).

In her research on the use of biometrics in the humanitarian sector, Zara Rahman (2018) concludes that in most cases the risks to refugees far outweigh the benefits. Acquiring biometric data presents many challenges, as biometric identification systems are often systematically biased against some ethnic groups. Fingerprint samples can be more difficult to collect for persons of darker skin colour or for people with disabilities, while fingerprinting can be inaccurate if beneficiaries' fingerprints are less pronounced due to manual and rural labour. Similarly, facial analysis software performs worse on darker skinned female faces than on any other faces, which may cause further obstacles to identification and access to services for refugees (Buolamwini and Gebru 2018).

False matches and unimagined repurposing of this data can also have consequences for refugees (as the case in Box 6 describes). False matches can happen when the quality of the data itself is not reliable, for example, with the changing shape of irises over time (Rahman 2018). These problems may pose serious harm to asylum seekers and refugees who may have their asylum requests denied or be turned away at the border because of a false match. There is little independent auditing and oversight to ensure equitable outcomes in these systems (Farraj 2010, 936).

[15] See European Union (2013).

[16] Biometric passports are equipped with an electronic chip that stores the individual's information such as their name, digital photograph, date of birth and other data.

Box 6: Case Study: Trace the Face Program

NGOs such as the International Committee of the Red Cross (ICRC) also use biometric data from asylum seekers and refugees. Their Trace the Face program uses facial recognition technology for FTR, by comparing uploaded “photos of missing migrants provided by their family with a current photo the person provided themselves” or by comparing “a photo of a migrant...[with] that of a possible blood relative, especially a sibling, parent, or child” (Bollag 2018). The program’s website does not give information about how these photos and information are protected. Furthermore, some of the files on missing persons on the Trace the Face website date back decades, and it is not clear whether the ICRC is using facial recognition technology on these photos as well.

There is also no information on the Trace the Face website regarding any process to obtain updated consent from family members, considering the technology may not have been used or even available at that time. When discussing this program with one of the refugees from Syria interviewed for this paper, they expressed concerns about matching photos of missing family members with images in the public domain: “Everybody is running away from the war, but some...are also running from family or someone who wants to hurt them.”

When false matches are made, the burden is often on the refugee to confirm their identity and prove that there was a mistake in the system. Because gaining access to the UNHCR services and aid is contingent on the biometric system working properly, any malfunctions could ultimately cause harm to an already vulnerable population. Errors could also limit or deny access to food, aid and important services, which is what happened to 6,500 Malian refugees in Mauritania in 2013, when there was a system malfunction in the biometric registration system (Radio France Internationale Afrique 2013).

The UNHCR has added to its handbook on data protection a section dedicated to explaining to data subjects exactly why biometric data, such as their fingerprints or an iris scan, is being taken, and what their rights are (UNHCR 2018). The language is similar to the rights of the data subject as outlined in article 29 of the EURODAC regulation. The asylum seekers and refugees interviewed for this paper, however, whose fingerprints were taken upon entry by law enforcement and border control agents in the European Union, said this explanation was not given during their registration.

> *They took our fingerprints when we arrived on the island [in Greece]. They said [that] only [the] border crossing was legal entry, and taking fingerprints was a normal procedure because we committed a criminal act. They also scanned copies of our passports, took photos of us, took our names and information. No one explained what they were doing with this information.*
>
> —Amin, 28, Syria

This lack of explanation and seeking of consent seems to perpetuate the stigma of criminality for asylum seekers, as Amin described. Although claiming asylum is legal and explicitly protected by international law, the European Union’s policy of taking fingerprints at the border, especially when done by force, can feel punitive to asylum seekers (Kroet 2015).

Refugees’ Right to Privacy

As non-nationals, refugees lack domestic legal data and privacy protections in their host country and must instead rely on international and regional legal mechanisms. The right to privacy has historically been one of the most difficult to define in a legal framework, due to not only its roots in cultural rituals, but also changing societal and political norms (Klitou 2014, 14). For asylum seekers and refugees, there are few options available for legal mechanisms that will protect their data and right to privacy.

Two major international human rights mechanisms that protect the right to privacy are the Universal Declaration of Human Rights (UDHR)[17] and the

[17] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III), online: <www.refworld.org/docid/3ae6b3712c.html>.

International Covenant on Civil and Political Rights (ICCPR).[18] Article 12 of the UDHR, ratified in 1948, defines privacy as individual autonomy, and identifies the right to demand protection of the law against arbitrary interference of privacy. Article 17 of the ICCPR builds on this UDHR language, and comprises a wider concept of obligations to protect privacy against interference and attacks from the government and others, without a limitation clause. The Charter of Fundamental Rights of the European Union (1951 Refugee Convention) offers refugees special protections.[19]

The EURODAC legislation currently under review would allow authorities to use fingerprints and facial images of children as young as six, and may be in violation of several parts of the UN Convention on the Rights of the Child (CRC).[20] The proposed legislation also permits use of coercion on children to obtain this data and is in violation of the CRC's article 19, which prohibits use of violence against children, and of article 22, which offers special protections to refugee children. The CRC also grants children the right to privacy in article 16, which the UN Committee on the Rights of the Child (2007, para. 64) defines, in cases of legal proceedings, "from the initial contact with law enforcement (e.g. a request for information and identification)" and may apply to taking biometric information from children.

Regionally, the right to privacy is also enshrined in article 8 of the European Convention on Human Rights. It provides a right to respect for one's "private and family life, his home and his correspondence," which are subject to certain restrictions "in accordance with law." Article 8 of the Charter of Fundamental Rights of the European Union more specifically outlines the right to protection of personal data: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[21]

Digital Agency and Informed Consent

Informed consent can be defined as granting permission with the full knowledge of possible consequences around the using, accessing or sharing of one's data, digital identities and online interactions (Lee and Tolvier 2017). Seeking consent and providing information about why data is collected supports the digital agency of refugees. There are several important components to the definition of "digital agency," first of which is a sense of ownership and control of one's own body and actions, as agency is defined in cognitive science (Jeannerod 2003). Secondly, agency can also be defined through a sociological lens as refugees' capacity to think, act independently, and make their own free choices. In sociology, agency is defined in contrast to structure, or outside influences, institutions, government, and policies that put limits on what individuals or asylum seekers and refugees can do, know, or control (Barker and Jane 2016, 280–82). Lastly, digital agency is defined through enabling information and communication technology users by providing them information they usually lack for making informed decisions (Kalantzis-Cope and Gherab-Martin 2010, 92–94).

There is often a big gap in technical literacy for some asylum seekers, such as Ali, who described how his fingerprinting and asylum application were not properly explained to him. In this case, not only did authorities fail to inform him that he was initiating the asylum application process, they also did not explain that the machine they were pressing his hand against was a fingerprint scanner — a machine he had never before seen (Reidy 2017).

> *I would say the biggest threat to Afghan refugees here is language. It took me a long time to understand what is the Dublin Regulation, and why I was sent back to Greece. I wanted to go to Norway, that's*

[18] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, at 171, online: <www.refworld.org/docid/3ae6b3aa0.html>.

[19] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, online: <www.refworld.org/docid/3ae6b3b70.html>.

[20] *Convention on the Rights of the Child,* 20 November 1989, 1577 UNTS 3, 28 ILM 1456 (entered into force 2 September 1990), online: <www.ohchr.org/en/professionalinterest/pages/crc.aspx>.

[21] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, online: <www.refworld.org/docid/3ae6b3b70.html>.

> *where I had some family, and I made it to Oslo after two weeks travelling. After some time, I applied for asylum in Norway to get papers and some kind of assistance. That's when they told me I have to go back to Greece, and they explained it's because I already applied for asylum. I remembered that they made me sign paperwork that was in English, and I spoke no English then. I didn't understand at all.*
>
> *They also put my hand on a glass box, it was very warm, I remember, I was afraid because I thought they would burn me. No one explained what it was. I didn't know that it was [for scanning fingerprints] and that they [can] find me with this anywhere in Europe. They should have said this to me first.*
>
> —Ali, 26, Afghanistan

In response to the surge of asylum seekers arriving to the European Union in 2015, a critical EURODAC regulation was passed as a security measure. The vast EURODAC database — including every person whose biometric data was recorded in the database — was made available to national law enforcement, border control and EUROPOL. The regulation also states that whoever refuses to have their fingerprints taken can, effectively, be forced to do so by means of coercion. It remains unclear how much force can be used (European Commission 2016).

The language of this regulation is alarming and further demonstrates the limitations on refugees' ability to exercise their physical and digital agency in this system. Asylum seekers are a particularly vulnerable group of people, with deep language barriers, who may have experienced trauma, post-traumatic stress disorder, persecution and state-sanctioned violence (Scherer 2015).

> *Once we arrived in Moria [refugee camp] they took us to registration. They said "Give us [your] fingerprints, this is to show you're legal for 6 months." I didn't ask who this is for, I just wanted to follow orders. I still have fear from my own police and military, and I didn't even think once to ask.*
>
> —Hadi, 26, Syria

The *UNHCR Handbook for Registration* states the need for accountability mechanisms that allow refugees to file complaints, make suggestions to improve the system, and report mistreatment or misconduct. However, it also requires the person filing a complaint to identify themselves. The lack of anonymity could act as a deterrent for some to speak up, especially if they fear retaliation and interference in their asylum application from the people the complaint was lodged against (UNHCR 2003, 135).

The UNHCR's policy on data protection lays out a procedure for personnel to notify the data controller of any personal data breaches and to properly record the breach (UNHCR 2015, section 4.41). However, it does not require them to contact the data subject affected unless the situation is deemed "likely to result in personal injury or harm to a data subject" (ibid., section 4.42). If this is the case, the data controller must notify the data subject and take mitigating measures as they see fit. This process is not specific; it does not offer any transparency or assurance to the data subject, considering the sensitivity of data stored. It also assumes the data controller is better equipped to judge whether the breach would cause injury or harm to the data subject, with limited information and understanding of individual risk.

The *UNHCR Handbook for Registration* (UNHCR 2003) is clearly geared toward humanitarian practitioners, as it misses key points of the process and is available only in English and French, which is not representative of the languages most refugees in the European Union speak. However, two of the refugees interviewed for this paper, who speak English as a second language, noted finding the registration handbook online while looking up information about their rights and how their data is processed and stored.

> *Everything I know about the process, and what is going to happen to us, I learned through Google. No one tells you anything. I got moved back from Germany to Italy because of [the] Dublin [Regulation], I didn't know about it back then. So, I started finding more information online, like the 1951 Refugee Convention online, and the UNHCR* [Handbook for Registration]*. It's good to have this online, but it's only in English.*
>
> *Everyone who travels here they must know their rights, what they have to go through, and this stuff. People come and they're quite ignorant how Europe works. In the beginning, when people are coming they need to know what the government is doing*

> *with this information, what they want to know about them and why. For some information the governments are asking, you can get killed for this information.*
>
> —Samir, 19, Somalia

Refugees in the digital age are able to coordinate their own movement through applications such as WhatsApp and Facebook, and may be aware of the potential surveillance risks these applications pose. Samir also explained how refugees search for information about their rights and data protection online, but even those materials do not offer many options for the millions of refugees who speak languages in which information is not readily available, such as Somali or Amharic.

A crucial part missing in guidelines for those seeking asylum is information about what does or does not constitute grounds for being granted asylum. This information is absolutely vital for an asylum seeker — knowing exactly what the interviewer is looking for would allow asylum seekers to properly explain those parts of their story or experience. Instead, it is almost as if it is assumed that those seeking asylum, if they had comprehensive information about the asylum process and the relevant laws and regulations, would give false information or abuse the system to act in their favour.

Information-Decision Gap

Being well informed of their rights about the data they are giving knowingly and consensually, through registration, is not enough for refugees and asylum seekers to be able to assess risks associated with how, and by whom, their data is stored and accessed. There remain concerns about future uses of collected data, data security risks and potential unintended consequences of data collection and storage.

Understanding How Data May Be Repurposed

The personal information and biometric data refugees share with authorities is sometimes used against them later, to detain or deport them if there are changes in administration or policies around asylum and security. For example, the EURODAC database itself has changed its permissions settings without the consent of the subjects whose data it made available to national law enforcement and EUROPOL in 2016 (European Commission 2016). Refugees learn about these policy changes and incidents online and then must take into account both what the potential threats of sharing this data might be for them and how the data might be repurposed.

There are many cases of migrants giving their information consensually for programs that promise them protection and rights, and later having that information used against them, when administrations and policies suddenly change. In the United States, 936,394 children of undocumented migrants applied for the Deferred Action for Childhood Arrivals (DACA) program under President Barack Obama’s administration. DACA gave new protections: a two-year period of deferred action from deportation; and eligibility for a work permit. Program participants were required to provide sensitive data in the application process, including their fingerprints, photographs, home address and educational history. Such sensitive information is now being used as a powerful weapon for surveillance, detention and deportations by President Donald Trump, who in 2017 announced plans to “phase out” DACA altogether (Pilkington 2017).

Refugees and asylum seekers may also be skeptical about sharing information with host governments. In 2006, then Minister of the Interior Nicolas Sarkozy collected information from families who were in France without papers, families with children in French schools and who demonstrated “a ‘real will’ to integrate,” promising them a path to residency and legal status (Murphy 2006). When only 6,000 out of the 24,000 who applied for regularization were given legal status and others were deported using the information they provided for the scheme, many perceived this as a way to trick migrants into giving the state information about themselves and the schools their children were attending (Pirot 2006).

Understanding Security Threats to Data Storage

Law enforcement and border control agencies also request access to the data of asylum seekers they suspect to be security threats from commercial actors such as Facebook, Google and Amazon. Asylum seekers' right to privacy is undermined through the sharing of big data with third parties. These companies all share data with law enforcement agencies, although the extent to which they act on court orders or simply respond to unwarranted requests from law enforcement agencies, including immigration agencies, is still unknown.

These companies have all also experienced major data breaches in recent years by hackers, including private sector actors such as Cambridge Analytica, who use data obtained without consent for media manipulation. Accurate information about data security breaches and hacking threats must be disclosed to data subjects; as well, data subjects must be informed that there are unknown digital threats to data protection. For example, in December 2017, a popular cloud storage service used by multiple UN agencies and several NGOs was hacked, and information about refugees was compromised (Parker 2017).

Breaches of data could also occur as the result of human error. In September 2018, it was revealed that OCHA accidentally published internal documents, passwords and access links to conference calls via a public project management application and "made sensitive material available online to anyone with the proper link" (Lee 2018). OCHA has since taken measures to secure accounts on external platforms they rely on, such as Google's G Suite and Trello, and has committed to developing practical tools to promote more consistent, responsible data practice within OCHA, stating, "Because documents [and project plans]...can contain sensitive information, it is important to use a trusted and secure tool and set appropriate access permissions when drafting them" (Centre for Humanitarian Data 2019, 26).

UN entities and their implementing partners have also been targets of government surveillance. The surveillance list of the United States' National Security Agency, which was leaked by Edward Snowden in 2013, revealed that the United Nations Children's Fund and Médecins du Monde were both surveillance targets (Glanz and Lehren 2013). Refugees, who have witnessed war crimes and come from countries such as Syria with sophisticated cyber intelligence operations, experience higher levels of risk in association with their data, thereby necessitating special and careful handling of this data.

How Is the Data Stored and Shared?

For EURODAC, all fingerprints collected from asylum seekers are sent and stored for up to 10 years in the Central Unit database in Brussels. The Central Unit is supervised by the European Data Protection Supervisor, while each EU member state is tasked with supervising the collection, use and processing of biometric data at the national level. The premises around the Central Unit database are secured with several layers of electric fences; 24/7 closed-circuit television and intrusion detection monitoring; security guards; and access control using fingerprints and personal badges.[22]

While EURODAC legislation currently has strict policies prohibiting sharing of data with third countries, provision EURODAC 2016/0132 (COD) will open the possibility to transfer personal data to third countries for return purposes, "if necessary in order to prove the identity of third-country nationals for the purpose of return" (EURODAC 2016/0132 (COD), art. 38.1). The UNHCR has been critical of this change, which will allow EURODAC to potentially give access to countries of origin that an asylum seeker has escaped from, in search of international protection (UNHCR 2016).

The UNHCR biometric database does not interact with EURODAC, although host countries can request the data from the agency. Arguably, the bigger problem for refugees is when the UNHCR shares data with host countries, who in turn share it with their countries of origin, as was the case with Rohingya refugees in Bangladesh. Refugees who refuse to give biometric data to the UNHCR are unable to receive assistance from the agency, thereby making the option of providing data a false one (Thomas 2018).

The WFP also shares information with governments, as well as with its partners and the private sector for research, without the consent or knowledge of beneficiaries. A 2017 internal audit found that the WFP also handles large amounts of personal data from beneficiaries without proper safeguards. The audit found that there were numerous data

[22] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (2017, 9).

protection failings across the WFP's data storage systems. The audit also found that unnecessary information was being gathered, including more personal information from beneficiaries than was needed, contrary to policy (Parker 2018).

For example, in 2017 the WFP conducted a study (Flaemig et al. 2017) with the University of Leiden, assessing the "digital footprint" of the WFP cash program. While the study produced a map tracking where refugees used e-cards for purchasing food items and how they moved around the country, there is no indication that beneficiaries were notified of or consented to the use and publication of their data, although the authors state that "appropriate data protection precautions were taken" and "should transactions analysis go into further detail...it is recommended to obtain explicit and informed consent from programme beneficiaries." In fact, the apparent disregard for consent in this particular study was amplified by a commenter asking if authors will share the full data set online, because a lot of data scientists "would be willing to work on problems and/or competitions to help solve humanitarian problems."

Those best intentions aside, if such data sets were to be published online, they could pose a significant threat to individuals, because they could be cross-referenced with other open-source data to identify individuals through open-source investigation techniques.

Refugees have found data sets exposing their information online without their explicit consent. It is therefore unsurprising that they may draw conclusions that their information may be shared with governments in their home countries too.

> *In 2012, in Lebanon, I was asked to register at UNHCR, but no more information was given to us about the process, what protection we have, what rights we have. No one contacted us after. I don't understand how the UN operates, to be honest. I don't trust the UN. I believe they share this information with the US and EU. It's possible they share this information with [the Syrian government], because they sometimes have research they publish on Syrian [refugees] in Lebanon — where they go, how they work, where they live. Their other information has been shared with the Syrian government, I'm sure of it.*
>
> —Amin, 28, Syria

> *I don't know what information the EU gives back to home countries. When I think about it, maybe the Afghan people who were deported back to Afghanistan, I imagine [the European Union] shares their files, they must. If that happens to Syrian refugees too, if it happened to me and I get sent back to war [motions cutting his neck with his index finger], I prefer to kill myself instead of letting them kill me. I have fear, I don't want to die. I want dignity, that's all.*
>
> —Hadi, 26, Syria

How Refugees Assess Risk with the Information They Are Given

In the absence of vital information about their data — which should be provided by institutions tasked with supporting them — asylum seekers and refugees have to rely on assessing risk based on rumours and information they can find online. Amin explained how another refugee was told that she would be deported back to Italy when she had claimed asylum in Sweden, and that there was a lot of conflicting information about what she needed to do to stay in Sweden with her child. Next, Rula described how rumours form in the Moria refugee camp on Lesvos about the asylum process, in the absence of proper information and consistent policy enforcement.

> *There is a community of refugees from different countries out here, we help each other out. One friend from Sudan entered in Italy, and she had to give fingerprints like me, and said it's because it's a crime to enter illegally. Later, in Sweden, she was told they have to go back to Italy — and she has a child also — and they said it's because Italy is their first point of entry to Europe. The other option was to leave the EU and come back after six months after your fingerprints are erased from the system, so they can apply for asylum again in Sweden. But how can they come back to Sweden like this, it's not possible. So, they went into hiding. It's*

> *happened to a lot of people, they are sent back to Greece, Czech Republic and Italy.*
>
> —Amin, 28, Syria

> *Some women [on Lesvos] even sleep on the beach, instead of [Moria camp], because they don't want to sleep in the same place as some men they don't know — you don't know what kind of things happen here. I am still waiting for my interview with the Greek Asylum to get [out of Moria camp], but I see people who arrived after me who get to leave before me, and also I see pregnant women, men in wheelchairs who should be sent to [the] mainland before any of us, and are still here waiting.*
>
> —Rula, 26, Syria

Providing asylum seekers with sufficient information about the asylum system and data that is being collected is insufficient in creating an environment where they feel in control of their own data and empowered to ask questions and lodge complaints when necessary. Certain factors, such as war trauma, cultural customs and obvious power imbalances between the interviewer and the asylum seeker, may prevent asylum seekers and refugees from asking questions and making complaints when they need to. Being in a situation where they have little power or agency, asylum seekers often avoid engaging in anything that can be seen as contesting authority or that could ultimately hurt their chances of being granted asylum.

Recommendations

Building the digital agency of refugees means not only advocating for enforcement of data protection policies and practices but also empowering asylum seekers and refugees through education — about how the asylum system works, how to control their information through data protection mechanisms and how to assess their own risks throughout the process. Based on the desk review and interviews conducted for this paper, the World Refugee Council, the UNHCR, the UNHCR's national implementing partners and other multilateral organizations should support and champion the digital agency of forcibly displaced persons by considering the following recommended actions.

Recommendation One: Informed Consent

Raising awareness about asylum seekers' and refugees' rights and the asylum process, and providing greater transparency regarding issues of privacy and consent, are vital to realizing the protection of asylum seekers and refugees. While asylum seekers may not object to the collection of their biometric data, existing processes and mechanisms fail to determine whether these individuals are provided with the requisite information to make an informed decision. Informed consent provides asylum seekers and refugees with a sense of dignity and respect.

> *Each country has their own process for asylum, it's a complicated system, and they make it complicated on purpose. I think the only way to make this easier for [asylum seekers] is if they sit down and explain the entire system to them — what information is important to say, why they ask for this information, who they will give it to, what might happen.*
>
> —Hadi, 26, Syria

Asylum seekers should be provided with legal education and information about their asylum claim options; the storage, use and access of the data they share; and their rights.

Recommendation Two: Regulatory and Legal Protections

Regulations to protect the rights of forcibly displaced persons, including asylum seekers and refugees, and to ensure greater transparency in the ways in which their biometric data is stored, shared and utilized, should be developed by UN agencies and NGOs to prevent further systemic marginalization. Gathering data through manipulation, pressure or coercion, such as through forcibly taking asylum seekers' and refugees' fingerprints, is not a consensual process.

EURODAC needs to explicitly give all the data subjects information about their rights, including the right to access, rectify and erase personal data and the right to lodge a complaint anonymously.

EURODAC and the UNHCR must ensure that data is freely given. The use of force should be explicitly prohibited by EURODAC in taking of fingerprints and other biometric data.

Recommendation Three: Access to Personal Data

Refugees and asylum seekers must have the ability to easily access and update their information; rectify mistakes or inaccurate data; and request that their information be deleted. Asylum seekers need to be able to request that their data be erased if they withdraw their asylum application or if their circumstances change in other ways.

Recommendation Four: Data Collection

Data collection must be minimized by all stakeholders, especially by smaller organizations that don't have strong internal data protection policies. Data collection should be used only in the specific ways the asylum seeker or refugee has consented to. For example, giving biometric data to the UNHCR does not mean refugees also consent to the sharing of their biometric data with host countries or their countries of origin.[23]

Humanitarian sector organizations must establish policies for gathering the minimum amount of data and must stop the processing of or erase data that is no longer necessary.

Recommendation Five: Curbing Techno-Solutionism in the Humanitarian Sector

Complex humanitarian problems merit careful analysis and multi-stakeholder engagement; they cannot be resolved with technical solutions alone. These challenges deserve nuanced, well-thought-out responses; careful analysis; community consent; and consideration of intended and unintended consequences. Many of the technology and data collection schemes developed by the UNHCR and its implementing partners lack a clear justification for their use and selection over other options. For example, there is currently no evidence on how useful biometrics have been in reducing fraud, creating opportunities for refugees or facilitating freedom of movement.

→ Donors should include data protection among their funding eligibility and reporting requirements and engage in open dialogue on the merits and impact of collecting various points of data.

→ The humanitarian sector should gather evidence and conduct research on the usefulness and feasibility of existing technologies being used for and by asylum seekers and refugees, and for and by the organizations and individuals tasked with supporting them.

→ UN agencies, in particular, should be transparent with the cost-benefit analysis of using biometrics and should define clearly how fraud is a problem for operations. The cost-benefit analysis should specifically compare the cost of running such a large-scale biometric program to the cost of fraud to the organization. The UNHCR and the WFP should also share evidence of supply chain fraud and fraud among field staff or partner organizations.

Recommendation Six: Engaging Refugees in Design and Problem Solving

Refugees are rarely consulted and engaged in developing solutions to the challenges they face. It is important to recognize the invaluable insights refugees and asylum seekers can provide on the issues and policies that shape their lives and to take note of the contributions they want to make and how they can utilize their skill sets. There is a tremendous amount of untapped potential within the refugee community — which includes designers, developers, social scientists, telecom engineers and others with valuable knowledge and expertise (among them are some of the individuals interviewed for this paper). For example, one person interviewed for this paper recommended working with refugees who have gone through the process recently to design clear visual guides that help asylum seekers and refugees navigate the asylum process and the biometrics and data required for each step of the process. They also suggested that such a tool might help authorities, the United Nations and NGOs operate more quickly if the asylum seekers know how to prepare and what to expect.

[23] For more on the FRIES consent framework as applied to personal data, see the Consentful Technology Zine at www.andalsotoo.net/wp-content/uploads/2018/10/Building-Consentful-Tech-Zine-SPREADS.pdf.

Organizations such as the Migration Lab, UNHCR Innovation Service and the Massachusetts Institute of Technology D-Lab engage the refugee community in development and design, thereby offering new and accessible socio-economic opportunities for them. Design that involves the most impacted communities is consistent with emerging best practices from the design justice framework for socio-technical systems (Costanza-Chock 2018). Co-design works best with a group that is diverse and representative of the refugee population.

Including minorities and marginalized groups from the refugee community in the decision-making and design process is crucial to addressing challenges in the asylum system faced by those who are the most vulnerable.

UN agencies and NGOs should post information about its programs and policies online in languages that refugees speak and understand.

Recommendation Seven: Compliance Mechanisms and Transparency

Humanitarian agencies lack incentives to share information on security breaches and missteps. Strong compliance mechanisms are needed to ensure better data protection and enforcement of protection policies. As well, it is difficult for asylum seekers and refugees to hold UN staff legally accountable for any malpractice because of the immunity afforded to many staff against major data protection mechanisms such as the European Union's General Data Protection Regulation. The individuals interviewed for this study have indicated that they would like an opportunity to express concern and ask for resources they are entitled to, without being afraid of how these concerns or requests will affect their asylum application and status. Refugees need to have a clear way to file a complaint against the organization or staff about their data internally, within the organization, to be able to hold them accountable for negligence or sharing their information without consent.

- → Data protection regulations from the United Nations and from national asylum agencies that collect and handle asylum seekers' and refugees' data should provide regular updates on evolving security threats and more structured procedures and guidelines for practitioners.
- → Funders and watchdog organizations must push for regular security audits that are shared with funders and the individuals who entrust them with their data.
- → The UNHCR must amend its policy of not accepting anonymous complaints in its *Handbook for Registration.*

Conclusion

Based on the desk review, discussions with UN and NGO staff, and interviews with asylum seekers and refugees, it is apparent that true informed consent may not be possible in the current EU asylum process, given the power dynamics at play between authorities and refugees. Stakeholders must acknowledge this power imbalance, and commit to seeking every opportunity to support the digital agency of refugees through legal education and participatory design and to access rights such as correction or deletion of one's own data.

One of the two major takeaways from this research was that the lack of transparency about the asylum process prevents asylum seekers from entrusting the system with the exact information that would likely win them asylum status. Mohamed described how he would not discuss sexual orientation and mental health illnesses with asylum officers because he felt it would lead to his application getting rejected, not knowing that that is the information officers need to give an applicant special protections. Samir also recalled meeting Somali women applying for asylum in Italy who did not want to tell the asylum officer about surviving sexual violence because of the stigma associated with it.

The second takeaway from this research was that innovation in the humanitarian sector may inadvertently be causing distrust within the refugee community and disrupting the asylum process. The best example of this from the interviews is when Amin had expressed clear distrust in the UN system after discovering research published online about Syrian refugees in Lebanon like him, used without their knowledge or consent. Another refugee from Syria expressed a lack of confidence in NGOs that use facial recognition technology, because of lack of regulation of protecting this data, and the lack of consent from the data subjects.

The lack of adequate education about the data collected quite clearly affects the asylum process, when asylum seekers do not trust the person taking information or feel comfortable sharing very sensitive data. Incorporating co-design in addressing challenges in the asylum system is an important step toward harm reduction and curbing techno-solutionism. Protecting personal data is integral to the "do no harm" ethos, as a humanitarian principle; transparent handling of data following the receipt of informed consent is key to building trust with this vulnerable group and to fostering greater digital agency.

Acknowledgement

This publication was made possible in part by a grant from Carnegie Corporation of New York. The statements made and views expressed are solely the responsibility of the author.

Works Cited

Asylum Information Database. n.d. "Reception and Identification Procedure: Greece." www.asylumineurope.org/reports/country/greece/asylum-procedure/access-procedure-and-registration/reception-and.

Barker, Chris and Emma A. Jane. 2016. *Cultural Studies: Theory and Practice.* 5th ed. London, UK: SAGE Publications.

Bellanova, Rocco, Maria Gabrielsen Jumbert and Raphael Gellert. 2016. "Give Us Your Phone and We May Grant You Asylum." *Peace Research Institute Oslo Blogs,* October 17. https://blogs.prio.org/2016/10/give-us-your-phone-and-we-may-grant-you-asylum/.

Bohlin, Anna. 2008. "Protection at the cost of Privacy — a study of the biometric registration of refugees." Master's Thesis, University of Lund.

Bollag, Burton. 2018. "Help me find my family." Devex, May 2. www.devex.com/news/help-me-find-my-family-92470.

Buolamwini, Joy and Timnit Gebru. 2018. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research* 81: 77-91.

Centre for Humanitarian Data. 2019. *OCHA Data Responsibility Guidelines: Working Draft*. March. The Hague, The Netherlands: OCHA. https://centre.humdata.org/wp-content/uploads/2019/03/OCHA-DR-Guidelines-working-draft-032019.pdf.

Costanza-Chock, Sasha. 2018. "Design Justice: Towards an Intersectional Feminist Framework for Design Theory and Practice." In *Proceedings of the Design Research Society 2018*, 529–40. www.drs2018limerick.org/participation/proceedings.

Council of the European Union. 2016. "EU-Turkey statement, 18 March 2016." Press release 144/16, March 18. www.consilium.europa.eu/en/press/press-releases/2016/03/18/eu-turkey-statement/pdf.

European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. 2017. *Annual report on the 2016 activities of the Eurodac central system, including its technical functioning and security pursuant to Article 40(1) of Regulation (EU) No 603/2013*. www.eulisa.europa.eu/Publications/Reports/2017-088_2016%20Eurodac%20Annual%20Report.pdf.

European Commission. 2016. *Proposal for a regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes*. COM(2016) 272 final, May 4. http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-272-EN-F1-1.PDF.

European Parliament. 2018. "Asylum: deal to update EU fingerprinting database." Press release, June 19. www.europarl.europa.eu/news/en/press-room/20180618IPR06025/asylum-deal-to-update-eu-fingerprinting-database.

European Statistical Office. 2019. "Asylum Statistics. Asylum applications (non-EU) in the EU-28 Member States, 2008–208." https://ec.europa.eu/eurostat/statistics-explained/index.php/Asylum_statistics.

Farraj, Achraf. 2010. "Refugees and the Biometric Future: The Impact of Biometrics on Refugees and Asylum Seekers." *Columbia Human Rights Law Review* 42: 891–942.

Flaemig, Tobias, Susanna Sandstrom, Oscar Maria Caccavale, Jean-Martin Bauer, Arif Husain, Arvid Halma and Jorn Poldermans. 2017. "Using big data to analyse WFP's digital cash programme in Lebanon." Humanitarian Practice Network, February 20. https://odihpn.org/blog/using-big-data-to-analyse-wfps-digital-cash-programme-in-lebanon/.

Glanz, James and Andrew W. Lehren. 2013. "N.S.A. Spied on Allies, Aid Groups and Businesses." *New York Times,* December 20. www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html.

Greece. 2016. *Law No. 4375 of 2016 on the organization and operation of the Asylum Service, the Appeals Authority, the Reception and Identification Service, the establishment of the General Secretariat for Reception, the transposition into Greek legislation of the provisions of Directive 2013/32/EC [Greece]*, 3 April 2016. www.refworld.org/docid/573ad4cb4.html.

Jeannerod, Marc. 2003. "The mechanism of self-recognition in humans." *Behavioural Brain Research* 142: 1–15.

Kalantzis-Cope, Phillip and Karim Gherab-Martin, eds. 2010. *Emerging Digital Spaces in Contemporary Society: Properties of Technology.* Basingstoke, UK: Palgrave Macmillan.

Kaurin, Dragana. 2016. "Migration." The Conference: Exploring Complexity in a Digital World, Malmö, Sweden, August 16. Video, 14:40 min. https://videos.theconference.se/dragana-kaurin-migration.

Kift, Paula. 2016. "In search of safe harbors — Privacy and surveillance of refugees at the borders of Europe." Association of Internet Researchers, Berlin, Germany, October 5–8. https://firstmonday.org/ojs/index.php/spir/article/view/8669.

Klitou, Demetrius. 2014. *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century.* The Hague, the Netherlands: TMC Asser Press.

Kroet, Cynthia. 2015. "Italy should 'use force' to fingerprint migrants." *Politico,* December 16. www.politico.eu/article/italy-should-use-force-to-fingerprint-migrants-frontex-refugees-dublin/.

Lee, Micah. 2018. "United Nations Accidentally Exposed Passwords and Sensitive Information to the Whole Internet." *The Intercept,* September 24. https://theintercept.com/2018/09/24/united-nations-trello-jira-google-docs-passwords/.Lee, Una and Dann Tolvier. 2017. "Building Consentful Tech." And Also Too, October 24. www.andalsotoo.net/wp-content/uploads/2018/10/Building-Consentful-Tech-Zine-SPREADS.pdf.

Meaker, Morgan. 2018. "Europe is using smartphone data as a weapon to deport refugees." *Wired,* July 2. www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations.

Murphy, Kara. 2006. "France's New Law: Control Immigration Flows, Court the Highly Skilled." Migration Policy Institute, November 1. www.migrationpolicy.org/article/frances-new-law-control-immigration-flows-court-highly-skilled.

Office of Internal Oversight Services. 2015. *Audit of the operations in Jordan for the Office of the United Nations High Commissioner for Refugees.* Report 2015/049. New York, NY: United Nations.

Parker, Ben. 2017. "Security lapses at aid agency leave beneficiary data at risk." The New Humanitarian, November 27. www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk.

———. 2018. "Audit exposes UN food agency's poor data-handling." The New Humanitarian, January 18. www.irinnews.org/news/2018/01/18/exclusive-audit-exposes-un-food-agency-s-poor-data-handling.Pilkington, Ed. 2017. "Dreamers' new risk after Daca: US could use their personal data to target them." *The Guardian,* September. www.theguardian.com/us-news/2017/sep/05/daca-dreamers-personal-data-undocumented-immigrants.

Pirot, Laurent. 2006. "Families Facing Deportation in France." Associated Press, August 14.

Purkey, Anna Lise. 2013. "A Dignified Approach: Legal Empowerment and Justice for Human Rights Violations in Protracted Refugee Situations." *Journal of Refugee Studies* 27 (2): 260–81. https://doi.org/10.1093/jrs/fet031.

Radio France Internationale Afrique. 2013. "Mauritanie: réduction des activités du HCR dans le camp de réfugiés maliens de Mbera." September 9. www.rfi.fr/afrique/20130909-mauritanie-le-hcr-reduit-activites-le-camp-refugies-maliens-mbera.

Rahman, Zara. 2018. *Biometrics in the Humanitarian Sector.* The Engine Room and Oxfam, March. www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf.

RefuComm. 2018. "Asylum in Greece — The Greek Sea Border — Reception and registration." Video, 7:34 min. YouTube, March 2. www.youtube.com/watch?v=_8yJQJpmAn8.

Reidy, Eric. 2017. "How a fingerprint can change an asylum seeker's life." The New Humanitarian, November 21. www.thenewhumanitarian.org/special-report/2017/11/21/how-fingerprint-can-change-asylum-seeker-s-life.

Scherer, Steve. 2015. "'No fingerprints!' chant migrants in Italy as EU cracks down." Reuters, December 17. www.reuters.com/article/us-europe-migrants-lampedusa-fingerprint-idUSKBN0U02H720151217.

Taylor, Diane and Emma Graham-Harrison. 2016. "EU asks tech firms to pitch refugee-tracking systems." *The Guardian,* February 18. www.theguardian.com/world/2016/feb/18/eu-asks-tech-firms-to-pitch-refugee-tracking-systems.

Thomas, Elise. 2018. "Tagged, tracked and in danger: how the Rohingya got caught in the UN's risky biometric database." *Wired,* March 12. www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh.

UNHCR. 2003. *UNHCR Handbook for Registration: Procedures and Standards for Registration, Population Data Management and Documentation*. Provisional Release, September. www.unhcr.org/en-us/publications/operations/4a278ea1d/unhcr-handbook-registration-provisional-release-september-2003-complete.html.

———. 2015. *Policy on the Protection of Personal Data of Persons of Concern to UNHCR.* May. www.refworld.org/pdfid/55643c1d4.pdf.

———. 2016. *UNHCR Comments on the European Commission proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the member state responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) — COM (2016) 270.* December. www.refworld.org/pdfid/585cdb094.pdf.

———. 2018. *Guidance on the Protection of Personal Data of Persons of Concern to UNHCR*. www.refworld.org/pdfid/5b360f4d4.pdf.

UN Committee on the Rights of the Child. 2007. *General comment No. 10 (2007): Children's rights in juvenile justice.* CRC/C/GC/10, April 25. www2.ohchr.org/english/bodies/crc/docs/CRC.C.GC.10.pdf.

About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan doté d'un point de vue objectif et unique de portée mondiale. Nos recherches, nos avis et nos interventions publiques ont des effets réels sur le monde d'aujourd'hui car ils apportent de la clarté et une réflexion novatrice pour l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

About the World Refugee Council

There are more than 21 million refugees worldwide. Over half are under the age of 18. As a growing number of these individuals are forced to flee their homelands in search of safety, they are faced with severe limitations on the availability and quality of asylum, leading them to spend longer in exile today than ever before.

The current refugee system is not equipped to respond to the refugee crisis in a predictable or comprehensive manner. When a crisis erupts, home countries, countries of first asylum, transit countries and destination countries unexpectedly find themselves coping with large numbers of refugees flowing within or over their borders. Support from the international community is typically ad hoc, sporadic and woefully inadequate.

Bold Thinking for a New Refugee System

The United Nations High Commissioner for Refugees (UNHCR) led a consensus-driven effort to produce a new Global Compact on Refugees in 2018. The World Refugee Council (WRC), established in May 2017 by the Centre for International Governance Innovation, is intended to complement its efforts.

The WRC seeks to offer bold strategic thinking about how the international community can comprehensively respond to refugees based on the principles of international cooperation and responsibility sharing. The Council is comprised of thought leaders, practitioners and innovators drawn from regions around the world and is supported by a research advisory network.

The WRC explores advances in technology, innovative financing opportunities and prospects for strengthening existing international law to craft and advance a strategic vision for refugees and the associated countries.

The Council will produce a final report grounded by empirical research and informed by an extensive program of outreach to governments, intergovernmental organizations and civil society.

À propos du Conseil mondial pour les réfugiés

Il y a en ce moment dans le monde plus de 21 millions de réfugiés, et plus de la moitié d'entre eux ont moins de 18 ans. En outre, de plus en plus de personnes sont forcées de quitter leur pays natal et partent à la recherche d'une sécurité, et elles sont alors confrontées aux limites importantes qui existent quant aux possibilités d'accueil et à la qualité de ce dernier. À cause de cette situation, les réfugiés passent maintenant plus de temps que jamais auparavant en exil.

En ce moment, le système de protection des réfugiés ne permet pas de réagir adéquatement à la crise des réfugiés d'une façon planifiée et globale. Quand une crise éclate, les pays de premier asile, les pays de transit et les pays de destination finale se retrouvent sans l'avoir prévu à devoir composer avec un grand nombre de réfugiés qui arrivent sur leur territoire, le traversent ou en partent. Et le soutien fourni dans ce contexte par la communauté internationale est en règle générale ponctuel, irrégulier et nettement inadéquat.

Des idées audacieuses pour un nouveau système de protection des réfugiés

Le Haut-Commissariat pour les réfugiés (HCR) des Nations Unies a dirigé des efforts découlant d'un consensus et visant à instaurer un nouveau « pacte mondial pour les réfugiés » en 2018. Mis sur pied en mai 2017 par le Centre pour l'innovation dans la gouvernance international (CIGI), le Conseil mondial pour les réfugiés (CMR) veut compléter ces efforts.

Le CMR vise à proposer une réflexion stratégique audacieuse sur la manière dont la communauté internationale peut réagir de façon globale aux déplacements de réfugiés, et ce, en se fondant sur les principes de la coopération international et du partage des responsabilités. Formé de leaders, de praticiens et d'innovateurs éclairés provenant de toutes les régions du globe, le CMR bénéficie du soutien d'un réseau consultatif de recherche.

Le CMR examine les progrès techniques, les occasions de financement novatrices ainsi que les possibilités pour ce qui est de renforcer le droit international et d'y intégrer une vision stratégique pour les réfugiées et les pays concernés.

Par ailleurs, le CMR produira un rapport final fondé sur des recherches empiriques et sur les résultats d'un vaste programme de sensibilisation ciblant les gouvernements, les organisations intergouvernementales et la société civile.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline