Big Data Surveillance Workshop, May 12th 2016

Refugees, Immigrants and Surveillance

By Monia Mazigh, The International Civil Liberties Monitoring Group

The migrant crisis with hundred of thousand of refugees fleeing war zones or waiting in refugee camps or arriving to new countries is a relatively new phenomena that the world didn't experience with this scale and intensity since the World War II.

But what is also most likely unprecedented is the new type of surveillance exercised by various governments to collect, store and share data about the refugees.

The refugees who are one of the most vulnerable groups in the world have today no choice than to accept that biometrics data, for instance, is collected and stored on their behalf.

Once biometrics data are gathered from refugees while they are in the refugee camps, waiting for their papers to be ready, it becomes more and more difficult to track down where the data will be sent and to who it will be transferred.

What the data is being used for? Will the data be shared with other agencies and foreign governments? How the data will be stored?

But biometric data is not the only new way to track down refugees and monitor them. Once, they arrive to the border of other countries, there are new technologies developed specifically to control them, push them away and close the doors at them. Drones, sensors, satellites are being developed and more and more used for those purposes.

Finally, once the refugees arrive to the countries they have been dreaming to be in, a whole series of measures will be waiting for them to spy on them, track them down an even detain them for indefinite time.

This paper will examine all the surveillance measures and tools that merged along with the waves of refugees who left their homes to arrive in their new countries.

1- At the refugee camp: the outgoing side

In 2011, when the first Syrian refugees started to arrive to Jordan, there were not enough installations ready to accept them and deal with their basic needs. However, in 2013, the United Nations High Commission for the Refugees (UNHCR) started using the ATM machines with biometrics data of the users in order to distribute relief money to the refugees.

Many of the asylum seekers who arrived to Jordan have never owned a debit card. The UNHCR created a new initiative to allow the refugees to access humanitarian aid money via ATMs that identify individuals by scanning their eyes.
There are about 633,000 Syrian refugees in Jordan and today, there are apparently 32,000 refugees participating in this program.

Collecting, storing and sharing data

Biometric data gathering is the collection of facial images, fingerprints and iris scans. These are highly personal data. The method requires such personal information to be given to the camp authority in order to receive financial aid.
The obvious argument of requiring such data from the refugees is to curb down fraud and criminal activities and that seems to be helpful. However, the refugees are in vulnerable positions, fleeing dangerous zones, and have no choice than to accept sharing this personal data with governments and international organizations. This is a new method to track down people and share their information with other governments.

The UN has said the program has greatly reduced fraud in the system; the number of Syrians requesting aid since iris scanning was implemented has reduced 30%. However, it is not clear for how long the UNHCR keeps the biometric data.

"If you have an active record, which means your registration is valid, and you're still an asylum-seeker, or refugee, the information is stored by default," said Volker Schimmel, head of Field Office Amman and manager of the UNHCR cash assistance program in Jordan. "Once the record is closed, we have data deletion protocols."

The official data protection policy of the UNHCR requires that the data shared with third party organizations should be deleted or destroyed once the partnership has ended.
The office in Jordan was audited and the result was unsatisfactory. Indeed, the list of beneficiaries (refugees benefiting the aid program) was sent to the bank on an encrypted CD. This is not the safest way to store and data. It can be hacked and tampered. The audit recommended that the personal data on refugees should be securely stored and transferred.

There are valid concerns about the data being shared willingly or accidently with Syrian authorities. In the context of the civil war, having information about refugees fleeing the country landing in the hands of the Syrian regime could be very dangerous in terms of political retributions either for the family members still living in Syria or the one who already left but are at the very high risk to be considered as traitors by the regime.

Biometrics is not only used for refugees from one country to another but also inside the same country to get information on migrants from rural areas to urban centres.

In India, 950 million citizens have participated in the government's biometric registration program. Around 200 million people, who arrived from villages to cities and who had never had identity papers, were tracked by the Indian government through biometric data. The government emphasized on the advantages of biometrics data for instance, the migrants who have no identity papers will be able to open for the first time bank accounts. However no measures were taken to protect the identity of these vulnerable citizens or to ensure that the privacy requirements are respected.
According to Anit Mukherjee, an International Development Research Centre fellow with the Center for Global Development, who worked as an early adviser to the project, the information collected by the government is never deleted. "Your biometrics live in the database for perpetuity," "It doesn't matter whether you're dead or alive."

The Department of Homeland Security in the United States published recently about the enhanced screening process for refugees.

Canada didn't accept any refugee coming directly from Syria. Canada accepts refugees already established in refugee camps in Jordan, Turkey or Lebanon and run by the UNHCR. Would that mean that the refugees who came to Canada shared their biometrics data with UNHCR and may be the Canadian government even before landing in Canada?

It should be mentioned that since last august 2015, the UNHCR does no longer require refugees seeking aid for biometrics data. The requirement has been replaced by informed consent. Moreover, the refugees are told about the data being collected about them and the whole process of using it and submitting it. Nevertheless refugees remain very vulnerable and privacy for some of the means nothing or very little.

Katja Lindskov Jacobsen, author of The Politics of Humanitarian Technology, argues that what seems like a choice in theory is, in practice, non-optional. "Either you give it, or you don't have assistance," Jacobsen said of biometric data. "I think that's the problem. European citizens can say no, if they want to."
Jacobsen said that states that collect biometric data have "national security" incentives that justify a level of secrecy around how that data is stored.

The UNHCR is under pressure from donor countries to embrace technological solutions to problems like fraud but meanwhile the data is being collected stored and shared with no safeguards and no accountability. Refugees have no legal right to know what happen to the data collected about them.

Recently, the UNHCR has introduced new changes to its biometric cash assistance program. The biometric data is no longer stored and transferred. The UNHCR uses a third party vendor called "IrisGuard". Refugees can now access cash from ATM, that scans the iris of the individual, creates a summary of the image, encrypts it and sends it via VPN (Virtual Private Network) to UNHCR server. After confirmation of the identity, the image is deleted and the information stored with the bank is also deleted. The UNHCR claim that in the future, the biometric data will be anonymously and aggregately shared.

These recent developments are an improvement in protecting the privacy of refugees but it is early to conclude that these vulnerable groups of individuals won't be taken advantage of while at the camps and whether the information collected on their behalf won't be shared with foreign countries on the receiving side.

Sources:

http://innovation.unhcr.org/labs_post/cash-assistance/
http://www.buzzfeed.com/carolineodonovan/tracking-refugees-puts-a-vulnerable-population-at-risk#.whRopNYqq

http://www.euractiv.com/section/justice-home-affairs/news/eurodac-fingerprint-database-under-fire-by-human-rights-activists/

https://www.uscis.gov/refugeescreening

http://www.rightrelevance.com/search/article
s/hero?article=0af255028e0478f81ae737407908deca39d61840&query=unhcr&tac
count=refugeerrights
...

2- At the border: the waiting area

Since 2013, when the migrant crisis started to become visible to the whole world, it was reported that many European defense companies started to offer their services to the European governments in the field of surveillance. This new focus emerged as a profitable opportunity for these defense companies as they have been struggling in the last years with defense budget cuts and fierce competitions.

Military technology – like satellites, sensors, and drones – are today being used to meet rising demands for border security.
"According to market analysis group Frost & Sullivan, the global border and maritime security industry was worth $29.3 billion in 2012. By 2022, that market is estimated to reach $56.5 billion."
The largest European defense players are Finmeccanica in Italy, the UK's BAE Systems, France's Thales, and European multinational Airbus, formerly EADS. Border control is already a core piece of these companies' export portfolios.
For example, from 2002 to 2013, Airbus, Finmeccanica, and Thales—largely through subsidiaries—have collected the lion's share of 225 million euros to thicken the defenses of "Fortress Europe" through the development of drones, olfactory sensors,

and border patrol robots.

It is hard to separate how much of these technologies have been used to track refugees and how much is being used for standard border operations.

- Europe’s big defense companies have assumed key roles on projects contributing to EUROSUR, a EU-funded surveillance system that uses drones, reconnaissance aircraft, and satellites to monitor Europe’s external borders. The European Commission estimates EUROSUR will cost 244 million euros between 2014 and 2020, though critics expect it will cost far more.
- “Perseus,” which integrates new and old sensor technologies on Europe’s seas and borders, is worth 43.6 million euros.
- “Seabilla,” a maritime surveillance project covering Europe’s Mediterranean, English Channel and Atlantic coasts, has cost 15.5 million euros.

There is a flagrant lack of accountability surrounding these security industrial companies. For instance there is no representative from migrant organizations or the UNHCR invited or consulted by the defense companies even if European governments are well represented.

Profits and competition remain the main motives behind these private companies. However, the new technologies they offer would be justified by the need of monitoring the borders or saving the refugees in distress.
Example: the use of drones in search-and-rescue operations in the Mediterranean Sea has been portrayed as a technology to rescue refugees but it is the same technology used to detect the presence of refugees at the borders.
Hungary is building a 175 km razor wire wall on its border with Serbia to keep refugees out.

But all these measures to fortify the borders won’t deter the refugees to cross the Europeans borders. All they do is that they raise the prices refugees had to pay to smugglers.
“Lots of money goes into border controls, but this does not address the causes of migration,” said Hein de Haas, a professor of migration studies at the University of Amsterdam and former director of the International Migration Institute at Oxford University. “Instead, it helps two groups,” he said. “The smugglers and the migration control industry, while the suffering and border deaths among migrants and refugees increase.”

Source:

http://fortune.com/2015/09/10/europe-migrant-crisis-defense-contractors/

3- In the new country: the receiving side

After the attacks of 9/11, it became so widespread that Canada is a “terrorist heaven”. The media, some experts and commentators and even some politicians kept this urban legend almost a “reality” on both side of the borders, despite the fact this is a false claim with no evidence to support it. According to Robert Leiken, a migration and security expert at the Center for the National Interest in Washington, "virtually everyone who has looked at the Canadian [refugee] system thinks it is the most relaxed, considerably more so than Europe."

For instance, it was widely mentioned in the media that the 9/11 hijackers entered the US though the “porous” Canadian border. In reality, all of the 9/11 hijackers entered the US in a legal manner using tourist and students visas.

Likewise, all the terrorist attacks or plots that happened or were stopped in Canada since the Air India bombing until the Parliament Hill and the Saint-Jean Attacks passing by the Toronto 18 plot, the alleged or convicted perpetrators were either established Canadian citizens or are legal visas holders.

In fact, the Canadian refugee system remains a very strict one, extremely hard to penetrate and the refugees arriving to Canada continue to be scrutinized in a very thorough manner.

The real question isn’t to know whether extremists or terrorists were able to fake their past and enter Canada but rather if any of these presumably terrorist were successful in conducting any violent or terrorist attack after entering Canada. According to *Andy Lamey is the author of* Frontier Justice: The Global Refugee Crisis and What to Do About It, there is only one documented case in the Canadian history that answers that question: the case of Essam Marzouki. He seems to be one of the only cases where a refugee who entered Canada and sought political asylum was later (after leaving Canada) allegedly found guilty of participating in terrorist attacks. Nevetheless, Mr. Marzouki didn’t use the Canadian refugee system to perpetrate a terrorist attack in Canada. The terrorist allegations against him happened later and in other countries and we are not sure at this point in time if they were proved in court.

The Security Certificates, CSIS and CBSA

The Security certificate is a mechanism by which the Canadian government can detain and deport a refugee or a resident permanent living in Canada, with the allegation that he represents a threat to the national security of Canada.

The evidence is collected by the Canadian Security Intelligence Service and shared with the Federal Court judge to review it. The main suspect is not allowed to see the evidence against him. Since 2008, a new regime of security certificate would allow a special advocate with a security clearance from the government to examine the evidence but won’t be able to share it with his client. This process remains problematic and several Muslim men have been subjects to security certificates since 2001.

In the case of Mohamed Harkat, even when he was released from prison, he had to be monitored by the Canada Borders Service Agency agents and had to comply with stringent restrictions of leaving the house or accessing the Internet. He constantly had to wear an electronic bracelet to monitor his mouvements and report them to CBSA.

In the security certificate cases, the interception of phone calls by CSIS and CBSA agents have been proved by lawyers of one of the man affected by the security certificate. In 2012, it was revealed that the phone calls of Mohamed Mahjoub and Mohamed Jaballah, both affected by security certificates, to their lawyers have been monitored by CSIS and CBSA.

Indeed, CSIS agents admitted to listening in on Mahjoub's calls with his lawyers in 2008. They claimed that they did so with the intent that the bail conditions are not breached.
However, the lawyers of Mahjoub argued that their client never agreed to allow the agents intrude the solicitor-client privilege. Despite, the security certificate, the lawyer and his client are allowed to speak on the phone without the CSIS or CBSA agents intercepting them.

Recently, it was reported in the British media that Immigration officials have been permitted to hack the phones of refugees and asylum seekers, for the past three years, since 2013. Many of them are rape and torture victims.
Those granted powers deal with "property interference, including interference with equipment". That means planting a listening device in a home, car or detention centre, as well as hacking into phones or computers.
Many civil liberties groups in the UK, are concerned that these powers would undermine lawyer-client confidentially privileges.
Immigrations officials claim that these powers are only used in "exceptional circumstances" to prevent crimes related to immigration cases but so far the parliament has not been able to review and reexamine these powers.

Sources:

http://www.theglobeandmail.com/opinion/canadas-refugee-system-is-a-dead-end-for-terrorists/article580517/

http://www.globaldetentionproject.org/countries/americas/canada

http://www.theguardian.com/world/2016/apr/10/immigration-officials-can-hack-refugees-phones?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+main+N

EW+H&utm_term=166283&subid=5135098&CMP=EMCNEWEML6619I2

Conclusion:

Since the day, they leave their villages, towns or cities, the refugees will be monitored through new measures, technological devices or equipment. Most of the time, these devices or technologies will be portrayed as tools to ease their suffering or make their settlement or stay more confortable and safer. It can be the case, but it can lead also to data being collected and transferred on their of refugees. It can lend them to prison and it can make their precarious lives at the camp more dangerous. Big Data Surveillance is affecting all groups and aspects of our lives and refugees are not immune of it. What make this issue a hard one is that refugees themselves do not have human groups who would fight for their privacy rights. They are in desperate need for food and shelter and safety that the data surveillance concerns seem to be a luxury not necessarily needed. Nevertheless, we strongly believe that every human being has the right to privacy and should be informed of his or her rights so no agency or government can take advantage of their vulnerabilities.