Smart Phones for Refugees: Tools for Survival, or Surveillance?

Photographs of refugees using smartphones have become common in the Western media landscape. Such images were much used to illustrate the arrival of refugees in Europe in 2015 and after. First stirring surprise, being at odds with stereotypes of refugees fleeing war, these images have now become more normalized. Using a phone or a smartphone has eventually become recognized as a matter of need rather than a luxury. What deserves public attention is that, along with this normalization, some European governments have taken an interest in how to make use of these devices and the digital traces of refugees (social media profiles, geo-tracking, etc). The ambition is to verify asylum seekers’ identity and to conduct security checks. In this policy brief, we review this emerging practice, and outline some of the key questions that it triggers.

Brief Points

- (Smart)phones are a much-used tool by migrants and refugees to find and share relevant information along the way.
- Several European governments allow – or seek new legislation to allow – the search of these devices and related digital traces in order to verify asylum seekers’ identity and run security checks.
- This raises a series of questions. Among them are the proportionality of such measures; the rights of the persons whose personal information is being searched; and, overall, the digital vulnerability of migrants and refugees.

Maria Gabrielsen Jumbert  
Peace Research Institute Oslo (PRIO)

Rocco Bellanova  
University of Amsterdam (UvA)

Raphaël Gellert  
Tilburg University
Smartphones have gone from being seen as a vital resource for refugees, to becoming a tool of surveillance regarding their background and entitlement to international protection. How did this shift come about?

**Smartphones: From Humanitarian Asset to Instrument of Verification**

Smartphones have been instrumental in the fight against identity fraud and falsification of asylum seekers’ files. The second purpose is to check whether migrants or asylum applicants constitute a potential security threat, where this form of surveillance is used more broadly as a counter-terrorism measure. In both cases, the underlying rationale is that smartphones and digital traces may unveil the real ‘truth’ about individuals.

The Belgian Secretary of State argued that up to 70% of asylum seekers lie concerning their situation in order to be awarded protection. He thus envisages the analysis of their digital devices as a kind of silver bullet solution, allowing relevant authorities to determine whether or not there is any falsification. While the German Interior Minister seems to rather emphasize the security-relevance of this new form of surveillance, the same assumption that digital devices may reveal a covered identity is at work.

**Digital humanitarianism and social sorting**

Whether in the service of humanitarian action or of security practice, what these devices ultimately contribute to is the emergence of digital refugees. Here, the digital may have a crucial role in the definition of a refugee’s life. A large part of the humanitarian discourse postulates that digital devices empower migrants, and this view seems to be in line with migrants’ own accounts of how they rely on smartphones during their journeys. However, what this discourse fails to properly acknowledge is that relying on digital devices means that people also become embedded into infrastructures that expose them to surveillance. A smartphone operates as a sort of gateway to many services, from the classical telecommunications to geolocalization and social networks. As such, it creates a vast amount of transactional information. These personal and meta-data can be used by governmental or other actors for the control purposes mentioned above, and can potentially be used to sort people
socially. Refugees are particularly vulnerable to these surveillance practices precisely because of their status as migrants. While they seek authorization to remain in Europe, European governments are trying to closely monitor and control the number of newly arrived migrants, and to sort between those with a legal right to protection and those who may not remain in Europe.

Some forms of control may also be wrapped in benevolent intent, such as providing necessary assistance to those in need. In facilitating access to digital devices and services, some actors, e.g. web developers or commercial businesses, may be interested in retaining a privileged position to harvest this wealth of digital data. Obviously, this is a practice that is nearly ubiquitous, where free online services are often set up in order to collect huge amounts of transactional data to be mined for diverse commercial purposes. However, when it comes to refugees, the dangers of data-leaks or misuses may have enormous consequences.

**Key Questions Raised by Use of Smartphones for Identity Verification**

Identity verification is a core concern of governments, but it is a tricky business. Fifteen years ago, the bulk of the debate over the securitization of asylum seekers was on testing their identity and tracking their movements through the capture of biometrics, with fingerprints becoming the key information to be fed into the EURODAC database. Back then, the refrain of public authorities was that “the body does not lie”. Nowadays, the tune seems to have changed to: “the digital device does not lie”. While fingerprinting and biometrics remain an important governmental technique to ‘manage’ human mobility, the smartphone is perceived as the gateway to people’s ‘digital selves’. The ambition is that identities can be inferred from people’s digital traces (network of contacts, messages stored, geolocalization, etc.). With the wealth of information shared and produced through the use of online platforms, there is a strong belief today in this giving access to the most accurate information about people’s identity.

In the following sections, we highlight questions that arise from the increasing practice of searching smartphones in the meetings between European authorities and persons seeking asylum in Europe. As an overarching principle, if the identity of persons fleeing wars and persecution would need to be verified with the help of smartphones, it is necessary to also assess and develop knowledge of how these devices are used. In other words, it is important not to be uncritical of the information they might provide us with. For instance, it has been reported that Facebook passwords have been commonly requested at checkpoints in Syria, both by governmental and IS forces, so as to identify people’s allegiance in the conflict. As a consequence, many users may have adapted or self-censured the content on their social media profiles and their phones in general, to distract from or avoid attracting unwanted attention. In some instances, the same device may also have been used, or is regularly used, by several persons, thus further unsettling the assumption that the transactional data generated pinpoint the true identity of a given individual. For governmental authorities, it is essential that the information potentially accessed is treated with caution and an understanding of the context in which the digital profiles and traces have been created.

**Effectiveness? Control measures affecting refugees and migrants**

A first question worth asking is whether this way of controlling migrants’ and asylum seekers’ identities is actually fit for a legitimate purpose. Such searching inscribes itself in longer trends of European authorities’ “need to use all information available” to have the best overview possible. Smartphones also come with the promise of giving access to a wealth of data, and thereby the assumption that they will ultimately provide more accurate information. Yet what is searched for and how the information is interpreted is what really matters. Further, as seen with other technologies aimed at controlling migrants’ mobility, they may eventually affect migrants’ (and smugglers’) behavior, as they adapt to this form of control.

It is important to question the ‘silver bullet’ expectation of some European governments that digital data may tell the ‘truth’ about individuals. The rationale that transactional data can be blindly considered legitimate ground to inform administrative decisions or judgments is too risky a shortcut.

**Proportionality? Assessing power dynamics and trust**

A second set of questions relates to the proportionality of this measure vs. the intended aim. There is an inherent power asymmetry between a European immigration official and the individual or family seeking to make a claim for
The right to privacy and data protection of refugees and migrants should not start only at the European border. Given the public/private nature of many humanitarian initiatives, and their transnational scope, the relevant legislative framework is often unclear. Privacy and data protection impact assessments may offer a framework to develop less surveillance-prone initiatives and infrastructures.

Overall, these governmental and non-governmental initiatives compel us to rethink our common and often simplistic tech-enthusiasm. They should invite us to start a more critical debate about how to reduce the vulnerability of digital migrants. A serious reflection on the implications of tech-based humanitarian assistance cannot be limited only to questions of privacy and data protection. Of particular concern are the implications of a hybrid form of governance, where private companies, state authorities, NGOs and international organizations fail to understand the surveillance capabilities of digital devices or fail to set high standards of digital safeguards. The use of multiple digital devices is set to become even more diffuse in the coming years. While they are key to providing access to wider systems, smartphones are but one of the many devices that populate migration spaces. In other words, the digital is no more a completely futuristic world, but rather part and parcel of the everyday of migrants. The possible implications for the persons concerned requires a view that is attentive to all migrants’ rights.

Along with the belief in the digital as delivering the most accurate information, it is also important to keep in mind that information found through such searches will also be interpreted; their meaning is not self-evident. This in turn raises the question of what will be the right to appeal for individuals concerned, also a key principle in European regulations on protection of personal data.

Privacy and data protection

Finally, data protection and privacy thinking can and shall intervene, especially when European agencies and governments consider accessing refugees’ smartphones. It should not be overlooked that the measures in question and discussed here are serious interferences with asylum seekers’ right to privacy. Following the well-established case-law of the European Court of Human Rights, the fact that such measures are explicitly provided for in a legislative provision is not sufficient to ensure their legality. One must also demonstrate their proportionality as well as the absence of less intrusive measures that would lead to the same result.

At the same time, the right to privacy and data protection of refugees and migrants should not start only at the European border. Given the public/private nature of many humanitarian initiatives, and their transnational scope, the relevant legislative framework is often unclear. Privacy and data protection impact assessments may offer a framework to develop less surveillance-prone initiatives and infrastructures.

Overall, these governmental and non-governmental initiatives compel us to rethink our common and often simplistic tech-enthusiasm. They should invite us to start a more critical debate about how to reduce the vulnerability of digital migrants. A serious reflection on the implications of tech-based humanitarian assistance cannot be limited only to questions of privacy and data protection. Of particular concern are the implications of a hybrid form of governance, where private companies, state authorities, NGOs and international organizations fail to understand the surveillance capabilities of digital devices or fail to set high standards of digital safeguards. The use of multiple digital devices is set to become even more diffuse in the coming years. While they are key to providing access to wider systems, smartphones are but one of the many devices that populate migration spaces. In other words, the digital is no more a completely futuristic world, but rather part and parcel of the everyday of migrants. The possible implications for the persons concerned requires a view that is attentive to all migrants’ rights.

Further Reading


