PRIO

PRIO POLICY BRIEF 04 2018

# 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*

Peace Research Institute Oslo (PRIO)
PO Box 9229 Grønland, NO-0134 Oslo, Norway
Visiting Address: Hausmanns gate 3

www.prio.org
Facebook: PRIO.org
Twitter: PRIOUpdates

ISBN: 978-82-7288-876-2 (print)
978-82-7288-877-9 (online)

## Smartphones: From Humanitarian Asset to Instrument of Verification

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?

### *Summer-fall 2015: smartphones and the 'refugee crisis'*

Images of refuges using smartphones were common in media coverage of the arrival of refugees in Europe during 2015. These images proved initially controversial. At first, the media coverage was centered on the very fact that many refugees then arriving in Europe actually had a smartphone. Responses soon followed however, mocking the European audience's ignorance for being surprised that refugees and migrants were 'connected people' too.

Then, as pictures of refugees using smartphones became more and more common, media commentators highlighted how these devices should be considered even 'more important' than water, food and shelter, due to their utility as tools to access information about where to find such resources when arriving in new places. Additionally, the fact that smartphones allow refugees to stay in touch – with each other and with family elsewhere – suggests that these phones have been important instruments for refugees' well-being and resilience. Various initiatives, from new volunteers to established humanitarian organizations, soon followed. Their aim was to equip refugees with digital devices or grant them access to relevant infrastructures, from power-banks to sim cards and Wi-Fi networks (see for instance Refugee Phones).

These initiatives, and the continued media coverage of the refugees arriving on Europe's shores, accompanied the emergence of a narrative of 'empowerment'. From this perspective, smartphones are *enablers*: they allow refugees to take care of themselves. In other words, the 'resilient refugee' is equipped with a smartphone, and humanitarian-like organizations (and even IT companies) should facilitate this form of empowerment.

Another underlying narrative, a sort of extension of the idea of the smartphone as a life-saving device, has portrayed the smartphone as a tool allowing migrants to cross dangerous borders. On the one hand, they may become less dependent on the "services" provided by smugglers – largely thanks to information exchanged on the best routes to follow. On the other hand, they may use phones to contact relevant authorities in case of danger, for example to call for rescue missions.

The encounter between smartphones and borders should have raised questions about the value of digital traces – and the devices that create them – for border guards and European authorities. Yet, while there were reports of police agencies using social media to get their messages and warnings across to the migrants through their smartphones, there was little critical assessment about how these easily transportable devices, storing large amounts of sensitive personal data about people who are often in very insecure positions, could also become a further source of vulnerability, and not purely an enabler and a tool of empowerment.

### *Summer 2016: smartphones, 'refugee status' and European security*

Then, on 29 June 2016, Belgian media announced that the Federal Secretary of State for Asylum and Migration, Theo Francken, intended to propose legislation to the Belgian Parliament that would allow Belgian immigration authorities to search asylum seekers' digital devices (like cellphones and laptops). The relevant legislation was eventually adopted in November 2017, despite the negative opinion of the Belgian Privacy Commission, which criticized the lack of clarity concerning data processing and data protection safeguards. The Belgian Secretary of State claims that such an initiative is made possible by the provisions of the European Union (EU) Directive 2013/32/EU of 26 June 2013 on "common procedures for granting and withdrawing international protection". Article 13.2(d) of this Directive states indeed that "the competent authorities may search the applicant and the items which he or she is carrying". Similarly, Thomas de Maiziere, the German Interior Minister, proposed the introduction of provisions permitting law enforcement authorities to access the smartphones and social media accounts of asylum seekers, in order to "make safety checks", i.e. carrying out identification in the absence of ID documents and searching for security-relevant information.

Similar new legislation, or extensions of existing laws, has been proposed in other European countries as well, including in Norway.

We can thus distinguish between two different, although related, purposes for searching smartphones and social media profiles. The first is to verify an asylum applicant's identity, and by extension verify whether they are entitled to the international protection they are seeking. Here, the rationale is that this information would be 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.

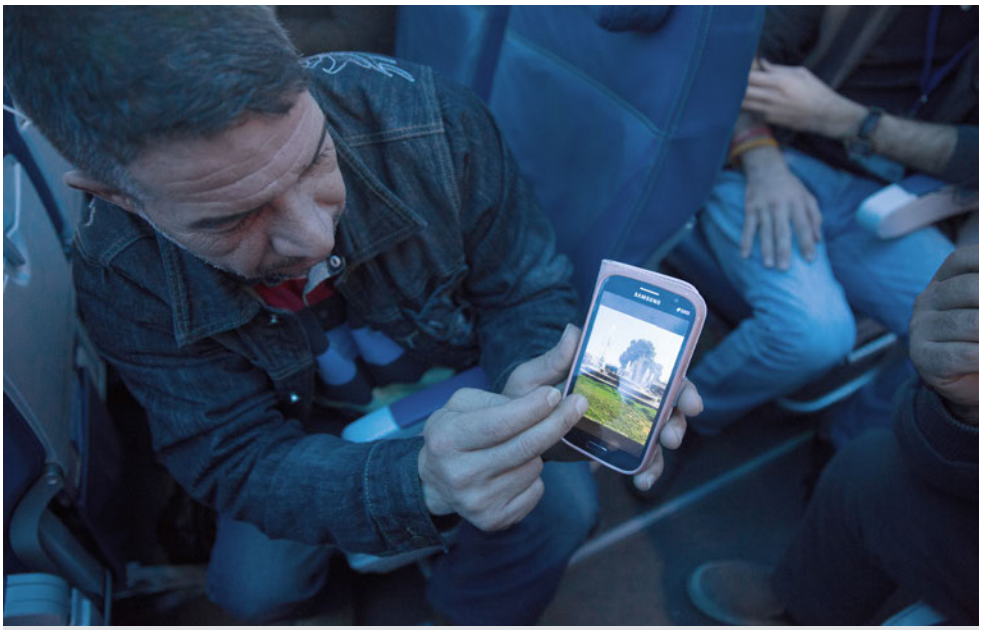
The Belgian Secretary of State argued that up to 70% of asylum seekers lie concerning their situation in order to be awarded protection. He thus envisages the analysis of their digital devices as a kind of silver bullet solution, allowing relevant authorities to determine whether or not there is any 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.



A Syrian refugee shows his home town of Hama on his phone while enroute to Canada. Photo: IOM / Muse Mohammed / CC BY-NC-ND @ Flickr

## 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

international protection. An important principle in EU law, and in connection with the right to protection of personal data, is the principle of proportionality. This requires that a limitation to this right must be justified; that any measure must be adequate in view of the actual objective; and only personal data relevant to the given purpose should be collected and processed.

Even where proportionality may be safeguarded, there is a possibility that measures seen as intrusive may affect the trust between refugees – persons in a vulnerable position – and the authorities. Some questions to address therefore include: Will the search of mobile devices be compulsory, or not? Will it be used for all asylum applicants, or only in cases where identity papers are lacking and in cases where there are serious suspicions raised against the applicants, in terms of security concerns?

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


Amicelle, A; C. Aradau and J. Jeandesboz (2015) 'Questioning security devices: Performativity, resistance, politics', *Security Dialogue* 46(4): 293–306.

Amoore, L. (2006) 'Biometric borders: Governing mobilities in the war on terror', *Political Geography* 25(3): 336–351.

Aas, K.F. (2006) 'The body does not lie': Identity, risk and trust in technoculture', *Crime, Media, Culture* 2(2): 143–158.

Broeders, D. and J. Hampshire (2013) 'Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe', *Journal of Ethnic and Migration Studies* 39(8): 1201–1218.

Chambers, P. (2016) 'Smartphone', in Mark B. Salter, ed. *Making Things International 2: Catalysts and Reactions*. Minneapolis: University of Minnesota Press, 195–215.

Jacobsen, K.L. (2017) 'On Humanitarian Refugee Biometrics and New Forms of Intervention', *Journal of Intervention and Statebuilding*: 1–23.

Kuner, C. and M. Marelli, eds. (2017) *Handbook on Data Protection in Humanitarian Action*. Brussels, Geneva: International Committee of the Red Cross.

Lyon, D., ed.(2003) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. London: Routledge.

Sandvik, K.B.; M.G. Jumbert; J. Karlsrud and M. Kaufmann (2014) 'Humanitarian technology: a critical research agenda', *International Review of the Red Cross* 96(893): 219–242.


## THE AUTHORS


Maria Gabrielsen Jumbert is a Research Director and Senior Researcher at PRIO. E-mail: margab@prio.org.
Rocco Bellanova is a post-doctoral researcher at the University of Amsterdam. E-mail: r.bellanova@uva.nl. Raphaël Gellert is a post-doctoral researcher at the University of Tilburg. E-mail: rgellert@uvt.nl.


## THE PROJECT

DIGICOM studies digitalisation in order to better grasp how new forms of risk communication affect societal security. It explores risk communication in different environments, such as authorities, news media and social media, as well as in relation to specific types of risk events that are of relevance for preparedness in Norway and beyond.

## PRIO

The Peace Research Institute Oslo (PRIO) is a non-profit peace research institute (established in 1959) whose overarching purpose is to conduct research on the conditions for peaceful relations between states, groups and people. The institute is independent, international and interdisciplinary, and explores issues related to all facets of peace and conflict.