The dangers and limitations of mobile phone screening in asylum processes

By **Kinan Alajak, Derya Ozkul, Koen Leurs, Rianne Dekker** and **Albert Ali Salah**

European authorities are increasingly screening asylum seekers' phones at the cost of their fundamental rights. In this piece, we suggest a procedural shift – prioritising fairness in the asylum procedure and voluntary cooperation towards purposeful goals.[1]

Asylum seekers use mobile phones for various purposes, including staying connected with their loved ones, planning their journeys, navigating travel routes, and securing housing and jobs. However, the dependence on mobile technology has also made asylum seekers particularly vulnerable to government surveillance, as their devices hold information about their movements and activities. European authorities are increasingly using data from mobile phones to gather evidence that can be used in decisions over asylum claims and, in some countries, to collect intelligence on migration-related crime and terrorism.

The practice of mobile phone screening has been severely criticised by civil society groups, including Gesellschaft für Freiheitsrechte[2] and Privacy International.[3] They argue that the practice is unlawful, invades privacy and lacks meaningful consent and safeguards to justify its necessity and proportionality. Moreover, the lack of transparency around data processing, the digital forensics software and the workings of algorithms used during the process could potentially undermine the fairness of the asylum procedure.

Despite these criticisms, several European countries persist in screening the mobile phones of asylum seekers. According to the European Migration Network's 2017 report,[4] mobile phone screening was standard practice in the Netherlands and Estonia, and optional in Croatia, Germany, Lithuania and Norway. In Latvia and Luxembourg, mobile phones were confiscated in the context of criminal procedures. Research[5] shows that data analysis of mobile phone content has been implemented in the Netherlands, Germany, Norway, and, to some extent, Denmark and the UK. Belgium, Austria and Switzerland have also amended their laws to permit such practices.

In this article, we compare findings from two similar studies conducted between 2021 and 2023 on the prevalence of mobile phone screening in Germany and the Netherlands.[6] The research team in the Netherlands filed Freedom of Information requests with the asylum authority *Immigratie en Naturalisatie Dienst* (IND) and the border police *Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel* (AVIM). They interviewed 13 state actors, civil society representatives, policy officers and law practitioners. In Germany, Derya Ozkul submitted several Freedom of Information requests to the Federal Office for Migration and Refugees - *Bundesamt für Migration und Flüchtlinge* (BAMF). Both studies also included interviews with individuals who underwent the asylum procedure. The team in the Netherlands interviewed seven individuals from Syria and Turkey, while the team in Germany interviewed eleven asylum seekers and refugees from Syria and Afghanistan. After providing a brief account of the screening practices in Germany and

the Netherlands, we argue that a number of flawed assumptions are being made based on 'data doubles' (profiles of individuals constructed from aggregated digital data) and discuss asylum seekers' reactions to the use of screening technology.

Mobile phone screening in Germany and the Netherlands

Immigration and border authorities in Germany and the Netherlands use mobile phone screening to identify asylum seekers and establish their country of origin. As part of this process, government officials confiscate the asylum seekers' mobile phones and other digital devices and either manually browse or automatically extract, analyse and use data from the phones during asylum assessments.

During our fieldwork, we found that both countries rely on private companies to provide them with hardware and software, support and maintenance. German authorities rely on Atos, a digital transformation-focused IT company that integrates products and services from two mobile forensic firms, MSAB and T3K-Forensics, to read and analyse data from electronic devices. In the Netherlands, the police produced their own software to automate data analysis, relying on companies like Cellebrite, an Israeli digital intelligence company, to supply the hardware (e.g., Universal Forensic Extraction Device "UFED") and software which extracts the data prior to analysis.

Despite many similarities in the practice, there are also some important differences. In Germany, the identification process is conducted as part of the asylum procedure, while in the Netherlands, it is conducted before an asylum application could be initiated. Therefore, in Germany, the analysis of phone data was the responsibility of the asylum authority, BAMF. In the Netherlands, however, the analysis of phone data was the responsibility of the border police (AVIM), not the asylum authority (IND).

The governing laws also differ. In the Netherlands, phone screening is covered under the Aliens Act 2000. Under this law, all adult asylum seekers are obliged to cooperate in a luggage search, a process which includes data carriers (including mobile phones and other digital devices). In contrast, in Germany, it is covered under the Asylum Act, and only those who do not have a valid passport or passport substitute are obliged to present their data carriers.

In the Netherlands, the main objectives of screening digital devices are to verify identities and collect signals related to national security. Therefore, information from the processing of data carriers could not be used by immigration authorities to verify asylum seekers' claims. Verification of someone's asylum claim was only recently proposed by parliament as an additional purpose, which would make smartphone screening part of the asylum procedure by the IND as well. In Germany, as the processing is part of the asylum procedure, the information obtained can be used more extensively in assessing asylum claims.

Common findings: mobile phone screening in practice

Mobile phone screening, as it is currently practised, violates fundamental human rights like those protected by Article 7 (respect for private and family life) and Article 8 (protection of personal data) of the Charter of the Fundamental Rights of the European Union, as well as Article 8 of the Convention. Yet, state authorities are permitted to carry out similar invasive practices under the same laws in the name of national security.

In both Germany and the Netherlands, the primary stated objectives of mobile

phone screening are verifying identities and registering asylum seekers. In the Netherlands, it is also stated to be directly related to safeguarding national security. When asylum seekers in both countries were asked about their opinion of mobile phone screening, most of them agreed with the objectives pursued by the state authorities. In the Netherlands, they were specifically concerned about war criminals receiving protection rather than facing justice for the atrocities they committed in their country of origin. In Germany, not all participants raised concerns about the practice, but none believed the process was the best way to achieve these objectives.

Our fieldwork identified several issues that indicate that mobile phone screening is an ineffective means of realising the stated objectives. This includes technical issues due to the data being unusable, limited or contaminated, and the risk that flawed assumptions will be made about individuals on the basis of the aggregated digital data about them. Asylum seekers have followed various tactics to avoid the invasion of their privacy and safeguard their rights.

Unusable, limited or contaminated data

In Germany,[7] only some of the extracted mobile phone data was found to be usable. Around a quarter of the readouts (23% in the first quarter of 2019 and 26% in 2018) failed on the technical level. Among the successful readouts, more than the majority (55% in the first quarter of 2019 and 64% in 2018) contained no useful findings. Out of those phones with usable data, only 1% of reports (i.e., only 12 cases) contradicted asylum seekers' submissions In the Netherlands, no technical failures were reported, but collecting intelligence for national security purposes, specifically to identify suspects of terrorism, did not yield any matches. In addition, the Dutch Council of State[8] advised that the law should more clearly define which purposes smartphone data can be used for and how long the data can be retained for, as smartphones contain large amounts of data, including personally sensitive data.

Besides technical failures, the effectiveness of mobile phone screening is naturally dependent on the availability of data. Limited data availability can occur when a mobile phone has been inactive for an extended period or when it has only been used briefly. This can be because asylum seekers are often afraid of the authorities and may choose to buy a new phone before facing them. This was observed among several of our interviewees in both countries.

For example, one respondent in the Netherlands, a 29-year-old Syrian female, shared:

> *"Honestly, people know that they do this, so they don't take their personal phones, you know. They take new phones like a fresh phone because I don't like other people to have access to my personal data in this way."*

Another respondent in Germany, a Syrian female in her 20s, shared that she bought a new phone before registration for asylum because she "did not trust that they would be spying on her and her private conversations and pictures". She only wanted "to get done with this [process] and decided to pay for another phone".

Moreover, mobile phone data itself may be contaminated. This may occur because multiple individuals use a single device, or an individual may use a second-hand device. Many asylum seekers we spoke to in Germany and the Netherlands used second-hand mobile phones and expressed their concerns about possible findings from previous owners of their mobile phones and

the risk of their asylum application being rejected as a result.

One respondent in the Netherlands explained:

> *"Maybe the phone you get is an old phone of – I don't know – someone committed war crimes. So, you are getting that, and now you are coming with that to the Netherlands. That would be a problem."*

In these cases, contaminated data can wrongly elicit authorities' suspicion towards applicants. In the Netherlands, applicants can be questioned in relation to national security, which may lead to them being denied the opportunity to make an asylum claim. Even if further investigation does not lead to denial, it is likely that the asylum procedure will be stalled. In Germany, applicants can be questioned further in the context of asylum processing. Unfortunately, identifying contamination in digital forensics remains a challenging task, which means applicants may be questioned unnecessarily, further hindering the fairness of the asylum procedure.

Misinterpretation of data contents

In cases where the available data is usable and not contaminated, the screening remains susceptible to the risk of state authorities' misinterpretation. For example, state authorities may challenge someone's stated country of origin because their mobile phone data shows the person had frequently called numbers in a different country, disregarding that the person may have several reasons for doing so. For instance, asylum seekers whose phone calls are inconsistent could have their family members residing in a different location than the stated country of origin.

A more problematic example is when state authorities disregard the cultural context and misinterpret the contents. For example, the existence of photos of weapons can lead to the person being associated with crime, whereas, as one of our participants explained: "in some places, pictures of weapons are considered a way of indicating someone's status." As such, misinterpretation can result when the dataset is taken out of context and used as a proxy to stand in for an asylum applicant's life story. This risk is exacerbated when smartphone data are extracted and analysed automatically without human intervention. The automation is part of the problem, but specifically the underlying biases embedded in the system warrant scrutiny.

In the absence of official information about mobile phone screening, asylum seekers take initiatives to safeguard themselves from potential accusations stemming from systematic biases, as another respondent, a 28-Syrian male, told us:

> *"When someone told me that they took our phones, the only alarming thing was to check my 1,000 friends on Facebook to check for any contact that could be, I don't know, it could be weird for them. Like, there are people, sometimes they change their photo to look manly, you know, like from the Middle East, and so… those I deleted. I didn't want to have any problem."*

Reacting to the perceived racial biases by authorities, our respondent deleted all his 'Middle-Eastern' looking friends with beards who 'looked manly'. However, these reactions may raise state authorities' suspicion of asylum seekers even further.

Misinterpretation during the processing of data carriers can also have unintended consequences on asylum claims. Authorities can doubt an applicant's claims if their phone data contradicts or does not provide enough evidence to support their statements. As an

example, an asylum seeker may be denied their application in Germany if their claim is related to being a member of the LGBTQ+ community and their phone data fails to provide sufficient proof. However, in certain countries such as Iran, Syria and Russia, Grindr, a popular gay dating app, is prohibited by law. Additionally, the cultural context plays a significant role. As one of our participants explained, in some countries, "people didn't dare to download Grindr or to keep personal, intimate photos on their phones" in fear of prosecution. In such cases, authorities may conclude, based on the absence of such apps or materials in the smartphone data, that there is insufficient evidence to grant asylum based on the person's LGBTQ+ status.

Conclusion

We have discussed the practice of mobile phone screening and showed that current procedures may undermine its effectiveness and legality. The practice assumes that a person's online activities can be used to verify their identity and support their claims without taking into account cultural context and technical limitations. Furthermore, mobile phone screening may violate asylum seekers' rights to privacy, protection of personal data, and a fair asylum procedure. We have also discussed asylum seekers' tactics to halt the practice and protect their privacy. Given the limitations to this practice, it is crucial to question why it is still being carried out. Future research should focus on evaluating whether the potential risks associated with phone screening and the stress it causes applicants are worth the cause, and whether upholding the 'human in the loop' principle which ensures data is interpreted by humans in its specific context may be a sufficient condition for mitigating systematic biases embedded in algorithmic decision making.

We propose a shift towards the voluntary provision of mobile phones to asylum authorities only if applicants deem them useful in support of their claim. This approach would respect their fundamental rights and ensure they are not subjected to unnecessary scrutiny.

Kinan Alajak
Research Assistant, Department of Media and Culture Studies, Utrecht University
k.alajak@uu.nl X: @KinanAlajak

Derya Ozkul
Assistant Professor, Department of Sociology, University of Warwick
derya.ozkul@warwick.ac.uk
X: @DeryaOzkul

Koen Leurs
Associate Professor, Department of Media and Culture Studies, Utrecht University
k.h.a.leurs@uu.nl X: @koenleurs

Rianne Dekker
Assistant Professor, School of Governance, Utrecht University
*r.dekker1@uu.nl X: @RianneDekker_*

Albert Ali Salah
Professor, Department of Information and Computing Sciences, Utrecht University
a.a.salah@uu.nl X: @SzassTam

1. *We are grateful for the work of Maarten Bolhuis, Evelien Brouwer and Mirjam Twigt whose scholarship informed this review. The findings cited in this piece have been gathered in the context of the Algorithmic Fairness and Asylum Seekers and Refugees Project funded by the Volkswagen Foundation and the Co-Designing a Fair Digital Asylum Procedure project funded by COMMIT and the Universities of the Netherlands.*
2. *bit.ly/refugee-phone-search*
3. *bit.ly/graham-wood-privacy-int*
4. *bit.ly/2017-emn-synthesis-report*
5. *bit.ly/automating-immigration-asylum*
6. *For more information about the case in the Netherlands, see Inspectie Veiligheid & Justitie. (2016, December 21). De Identificatie van Asielzoekers in Nederland. Vervolgonderzoek naar de registratie en identificatie van asielzoekers door politie en Koninklijke Marechaussee. Ministerie van Justitie en Veiligheid, Den Haag. For the case in Germany, see Biselli, A. and Beckmann, L. 2020. Invading Refugees' Phones; Palmiotto, F. and Ozkul, D. 2023. "Like Handing My Whole Life Over": The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures, VerfBlog, 2023/2/28.*
7. *bit.ly/invading-refugees-phones*
8. *bit.ly/government-gazette-netherlands*