Seeking asylum in the digital era

Bolhuis, Maarten; van Wijk, Joris

published in
Journal of Refugee Studies
2021

DOI (link to publisher)
10.1093/jrs/feaa029

document version
Publisher's PDF, also known as Version of record

citation for published version (APA)
Bolhuis, M., & van Wijk, J. (2021). Seeking asylum in the digital era: social-media and mobile-device vetting in asylum procedures in five European countries. *Journal of Refugee Studies*, *34*(2), 1595-1617. https://doi.org/10.1093/jrs/feaa029

Journal of Refugee Studies Vol. 0, No. 0 © The Author(s) 2020. Published by Oxford University Press.

doi:10.1093/jrs/feaa029

Seeking asylum in the digital era: social-media and mobile-device vetting in asylum procedures in five European countries

MAARTEN P. BOLHUIS

Department of Criminal Law and Criminology, Faculty of Law, Center for International Criminal Justice, VU University, The Netherlands
m.p.bolhuis@vu.nl

JORIS VAN WIJK

Department of Criminal Law and Criminology, Faculty of Law, Center for International Criminal Justice, VU University, The Netherlands

MS received July 2019; revised MS received February 2020

The increasing use of social media and mobile devices by asylum seekers offers new vetting opportunities for immigration authorities, to verify the identity or to assess national-security or 1F-exclusion aspects. Based on interviews with practitioners in Belgium, Germany, the Netherlands, Norway and Sweden, the first experiences with both of these new methods seem to be mixed, while formal evaluations of the results seem to be lacking. We argue that the increasing reliance on these methods, in combination with the further advancement of technology, raises important questions about possible infringements on the right to private life, as well as the risk of function creep and social sorting. It can be questioned to what extent the use of these new vetting tools and methods is proportional to the results they produce and to what extent fundamental human rights, including privacy, are sufficiently safeguarded.

Keywords: social media, smartphones, asylum, surveillance, Article 1F

Introduction

Social media and mobile devices (smartphones, tablets, laptops and other portable digital data carriers) have become almost indispensable tools for migrants, including asylum seekers. Recent studies on their use of social media suggest, for instance, that the majority of Syrian asylum applicants have used social media prior to and during their migration to Europe (Emmer *et al.* 2016; Gillespie *et al.* 2016; Dekker *et al.* 2018). By providing access to information and a means for navigation and communication, social media and mobile devices shape the decision-making on travel routes, travel methods and final destinations, they make migrants more autonomous and less reliant on smugglers or traditional migration

network ties, and could enhance migrants' safety by enabling them to contact authorities in case of danger (Dekker and Engbersen 2014; Dekker *et al.* 2016; Zijlstra and Van Liempt 2017; Alencar *et al.* 2018; Dekker *et al.* 2018; Jumbert *et al.* 2018). In fact, it has been argued that social media is transforming migration networks, thereby lowering the threshold for migration (Dekker and Engbersen 2014), even though a 'digital divide' still exists: not all nationalities, communities, ethnicities, sexes or age groups have the same access to information and communication technologies (Hamel 2009). Smugglers also make use of social media for advertising their 'services' (EMN 2016b; Europol/EMSC 2017; Hacsek and Visnansky 2017).

While the increasing use of social media and mobile devices is believed to facilitate unauthorized migration, and thus potentially help increase its volume, they also offer (immigration) authorities in receiving countries new opportunities to communicate with (prospective) migrants prior to and during their journey, for example by offering 'counter-narratives' (EMN 2016a)—or, one could say, *deterrence* narratives—that detail the dangers of illegal border crossings or provide factual information about (the difficulties of getting) access to residence permits, work or allowances (although the effectiveness of such campaigns can be questioned; see Schans and Optekamp 2016). Additionally, and this is what this contribution will focus on, the increasing use of social media and mobile devices by asylum seekers also offers new vetting opportunities for immigration authorities. Social-media activity, open-source information on the Internet and the content and geodata on mobile devices can potentially be used to verify or debunk claims made by asylum applicants about e.g. their identity, country of origin or travel route. Since information that is collected for one objective can also be relevant for other objectives, such information could furthermore be used to assess whether applicants pose a threat to the national security or should be excluded from international protection on the basis of Article 1F of the 1951 Refugee Convention. For example, data carriers may contain (photographic) evidence of crimes forwarded to, witnessed by or perpetrated by the applicant. While a picture in itself is not necessarily sufficient to have any direct repercussions for the assessment of an asylum claim, such information can in any case be a reason to ask the applicant to explain what was found.

Building upon our previous work (Bolhuis and Van Wijk 2018, 2019), this article discusses whether, to what extent and how European immigration authorities are analysing activity and content on social media and mobile devices for the purpose of (i) establishing and verifying the identity of asylum applicants and (ii) screening on national-security or 1F-exclusion indications. It maps and describes these practices in the context of asylum procedures in five European countries that dealt with a substantial increase in the number of asylum applications from 2015 onwards: Belgium, Germany, the Netherlands, Norway and Sweden. What exactly is defined as a threat to 'national security', or to the 'security of the state', differs from country to country, but is often based on the alleged involvement in serious (most notably terrorist) crimes (EMN 2016a).

After outlining the methodology and providing relevant contextual information about identity, national security and 1F refugee exclusion vetting during the heightened asylum influx in Europe from 2015, based on a literature study and expert interviews, the article will first discuss two empirical questions: (i) what screening and analysis of social-media profiles and mobile devices are immigration authorities in Europe currently conducting and (ii) what are the results? In the final section, we will contextualize the presented empirical information by critically discussing the legal, normative and societal implications of these new vetting tools. Based on, inter alia, insights from 'crimmigration', big data and privacy literature (Stumpf 2006; Brouwer 2011; Van der Woude *et al.* 2017; Privacy International 2019), we argue that the increasing reliance on these methods, in combination with the further advancement of technology, raises important questions about possible infringements on the right to a private life, as well as the risk of function creep and social sorting. It can be questioned to what extent the use of these new vetting tools and methods is proportional to the results they produce and to what extent fundamental human rights, including privacy, are sufficiently safeguarded.

Methodology

This article is based on a combination of expert interviews and a review of available academic literature, relevant rules and regulations, and available formal and informal policy documents. The most substantial part of the research was conducted as part of a research project funded by the Norwegian Directorate of Immigration, the UDI (Bolhuis and Van Wijk 2018).

In the context of the mentioned project, between November 2017 and May 2018, interviews were conducted with a selective sample of 43 representatives of immigration authorities and aliens police agencies in the five focus countries, as well as representatives of intelligence and security services and representatives of the European Asylum Support Office. In the context of this article, especially the following immigration authorities and aliens police agencies in the five focus countries will be referred to: the Office of the Commissioner General for Refugees and Stateless persons (CGRS) and the Immigration Office (DVZ) in Belgium; the Federal Office for Migration and Refugees (BAMF) in Germany; the National Police's Department of Aliens, Identification and Human trafficking (AVIM) and the Immigration and Naturalisation Service (IND) in the Netherlands; the National Police Immigration Service (PU) and the UDI in Norway; and the Swedish Migration Agency (SMA) in Sweden. Through the researchers' existing network and with assistance from the UDI, key respondents were selected in the initial phase of the research. Once contact was made, additional respondents were approached using snowball sampling. All envisioned respondents were approached by either email or telephone with the request to cooperate in this study. They were informed that the data they provided would be used in a report on behalf of the Norwegian government and subsequently written academic publications, that their anonymity would be guaranteed and that the findings would be made publicly available in the English language. When the approached respondents accepted

the invitation, where possible, the interviews were conducted face to face. All interviews had a semi-structured character and generally lasted for an hour up to 3 hours. The interviews were not audiotaped, but transcripts of the interviews were made during and directly after the interviews. These transcripts were shared with the respondents for approval. Respondents were asked to check whether the transcript was factually correct and/or to provide additional information.

In addition, the authors gathered and analysed relevant academic literature, policy documents, and rules and regulations on the identification and registration of asylum seekers, asylum procedures and screening activities related to national-security and 1F-exclusion cases, including information from two studies conducted by the European Migration Network (EMN 2017a, 2017b). Finally, an expert meeting was organized at the Center for International Criminal Justice in Amsterdam on 17 April 2018, entitled 'Screening and Identification of National Security and Exclusion Aspects in High Asylum Influx Situations'. Six experts from Belgium, the Netherlands and Norway participated in the meeting. All of them were working in the asylum process and had specific expertise on matters of national security and exclusion. In this article, respondents and participants in the expert meeting are referred to with codes R# and E#, respectively.

The 2015 Asylum Influx and Issues of Identity, National Security and 1F Exclusion: A 'Perfect Storm'

In terms of identity establishment or screening on national-security or 1F-exclusion indications, the 2015 high influx of—in particular Syrian—asylum seekers could be considered a 'perfect storm'. Still picking up the pieces of the 'economic crisis' and after having had a relatively low and stable influx of asylum seekers for years, European governments were suddenly confronted with a very substantial number of newly arriving asylum seekers from an active battlefield where numerous war crimes and crimes against humanity were committed by all parties, including designated terrorist organizations openly challenging the Western world. Intelligence and security services perceived these asylum seekers to pose a serious security threat and, in various European countries, immigration authorities were pressed by politics and media to raise awareness and alertness on war criminals and terrorists arriving in Europe by making use of the asylum system (Bolhuis and Van Wijk 2018).

Although, for the largest group of asylum applicants—those of Syrian origin—lacking documentation represented less of a problem than with groups of other origins (*ibid.*: 73), the reliability of Syrian identity documents was questioned by European immigration authorities. From September 2015 onwards, reports emerged that legitimate Syrian passports were issued by Syrian embassy offices with 'virtually no checks' (Dawar 2015); that fake passports were widely available on the black market (Ezadi 2015); and that the Islamic State (IS) had obtained a substantial number of blank passports as well as passport-printing machines after seizing Syrian government assets (Marsh 2015). Because of these developments, authorities could no longer rely on apparently legitimate documents to definitely establish whether someone actually held Syrian nationality. An additional

challenge in this context was that Syrian asylum applicants basically only needed to make it credible that they were Syrian to be granted asylum; therefore, compared to asylum seekers with other nationalities, much less information from asylum interviews was available to assess whether an applicant had anti-Western sentiments or had been involved in crimes. Furthermore, because of the large numbers of asylum applications, relatively little time and few experienced staff members were available for investigations (Bolhuis and Van Wijk 2018).

What facilitated, but also complicated, the identification of possible war criminals and terrorists was that an unprecedented body of information was available. Various respondents referred to Syria as the 'best documented conflict ever'. At the same time, it could be considered the 'most messily documented conflict ever'. Not only did established Western organizations such as Amnesty International, Human Rights Watch or the International Crisis Group publish formal reports, in addition also Arabic news outlets, the warring parties themselves, bloggers and citizen journalists posted an unparalleled number of online articles, videos and blogs about the conflict and the resulting refugee flows. In addition, there was increased pressure to screen social-media accounts because journalists, activists and interest groups, on the basis of social-media searches, started publishing information about the alleged criminal background of asylum seekers in Europe on dedicated websites. Evidence of the commission of serious crimes in the Middle East was available for analysis almost in real time, sometimes distributed by the perpetrators themselves, sometimes tampered with or forged. Immigration authorities had to develop strategies, routines and protocols on how to deal with this profusion of data. In addition, many of the relatively well-to-do Syrian asylum seekers who entered Europe were active social-media users and arrived with smartphones and computers that contained an abundance of—possibly relevant, but also much irrelevant—information. The context in which European immigration authorities had to assess asylum claims was complex and challenging. Within a short time frame, they were confronted with a large group of asylum seekers from the Middle East, while there was much political and societal pressure to critically assess whether these applicants posed a threat to national security. Because of the increased use of social media and data carriers, there was an abundance of information available to analyse: how to go about it?

Social-Media and Mobile-Device Analysis in Europe

In the challenging environment described above, analysing content from social media and mobile devices has become increasingly relevant for immigration authorities. This paragraph describes to what extent and how these methods are used and what is known about their results.

To What Extent and How Is the Method of Social-Media Analysis Used?

The synthesis report of a 2017 study performed by the EMN into practices in establishing the identity of asylum applicants notes that the analysis of publicly

accessible social-media content became standard practice in recent years in inter alia Belgium, the Netherlands and Norway as well as two other EU Member States, while it is optionally used by 11 other Member States, among them Sweden (EMN 2017b: 32). The increasing use of social-media research seems to be unrelated to the *scale* of the high influx from 2014 and can rather be explained by the advancement of technology and by the *nature* of the influx, namely the fact that, in particular, Syrian asylum seekers were relatively active on social media and often had smartphones at their disposal compared to asylum seekers from other countries (R31, R32, R34, R35). Arguably, the interest in using social-media analysis was not only given by the new possibilities that it offered to check someone's identity. As mentioned above, there was also increased pressure to screen social-media accounts because journalists, activists and interest groups, on the basis of social-media searches, started publishing information about the alleged criminal background of asylum seekers in Europe on dedicated websites.

Our study confirms that, except for Germany, in all of the other four focus countries, immigration authorities use this kind of analysis, for the establishment of identity as well as for screening on national-security and exclusion indications. In 2018, the German BAMF informed us that it was exploring possibilities for conducting social-media analysis in the future, but that it had thus far not been using the method (R38). Whether the method is used in all cases or selectively differs between the countries. In the Netherlands, the IND conducts an analysis of social media and other open-source information in all cases, as part of a separate procedural step referred to as 'screening', which was introduced in March 2016. In the other three countries, social-media analysis is conducted selectively. In Belgium, social-media analysis is only conducted by the CGRS in cases in which there are certain indications or doubts about the information provided by the applicant; according to respondents, the choice of such a selective use of social-media analysis was made in particular because the method is time-consuming (R22, R23). In Norway and Sweden, individual caseworkers of the UDI and SMA decide whether or not to use the method. A UDI representative indicated in this respect that whether the method was used mainly depended on the familiarity of the caseworker with social media; younger caseworkers would use it more often than older caseworkers. However, from the end of 2016, social-media analysis started to be applied more systematically by the UDI (R7).

In the four countries, social-media research is generally conducted by regular caseworkers, who typically have been provided with some guidelines, instructions and training on how to conduct social-media research. In the Netherlands as well as in Sweden, they are for example instructed not do social-media vetting with a private computer or a private account (IND 2016; R43). In Belgium, this guidance seems to have taken the most concrete form. As part of a special project on the implementation of the use of Facebook for social-media research, the Belgian CGRS has established a specialized unit falling under its country-of-origin information desk. This 'New Media Unit' provides continuous training to caseworkers on how to engage in social-media research. Next to providing guidance and training, the unit also assists caseworkers in carrying out actual social-media research;

it for example has staff members who read Arabic and Russian and may take on 'difficult' cases such as 1F-exclusion cases (CGRS 2017). Similarly, Sweden and the Netherlands have specialist teams that can assist caseworkers in (using social media in) possible exclusion or national-security cases (R31, R43).

As caseworkers of the immigration services only use information that is publicly available, in principle, cooperation from the applicant is not required. An applicant could, however, be asked specifically to disclose information on social media that may be relevant to the asylum application. In Belgium, an amendment of the Immigration Act created the possibility for the CGRS to 'invite' the applicant to submit any relevant information on social media in case there are any suspicions that he or she withholds information (EMN NCP Belgium 2017: 40). Refusing to disclose information on social media can be taken into account in deciding upon the application, when there are other indications that may possibly be a reason to deny the application. Refusing to cooperate in this sense may also be a reason to ask the intelligence services for information (R20).

Training available online by a social-media analysis specialist from the Belgian CGRS gives a good idea about some of the practical problems encountered in social-media analysis by immigration authorities, as well as some of the techniques and tools to overcome these problems (CGRS 2017). In line with the remarks from the CGRS specialist in this training, several respondents noted that, if social-media analysis—or, for that matter, even a simple online search—is performed in an ad hoc or incautious manner, this may have severe consequences for the confidentiality of the asylum procedure and may even be illegal. For instance, a respondent of the Norwegian PU gave the example that, when caseworkers would type in the name of applicants in a search engine from their offices with the goal of obtaining more information on these individuals, this search engine could easily register from which address the search for this particular name is conducted. Consequently, this may create possibilities for third parties, such as the authorities of the applicants' country of origin, to identify in what country the individual applied for asylum. For this reason, the respondent warned that only authorities with the right expertise should be engaged in social-media analysis (R12). Swedish and Dutch respondents also acknowledged that probing into a case of someone in need of protection by the immigration services might leave traces, which carries the risk of impeaching on confidentiality (R28, R31, R32). For this reason, the Dutch IND uses standalone computers with special software and special accounts to safely perform open-source and social-media research. These 'Internet detective network' (iRN) computers have been developed by the Dutch National Police in collaboration with a commercial cyber-security company (R31, R32).

To What Extent and How Is the Method of Mobile-Device Analysis Used?

Apart from social-media analysis, another development that coincided with the high influx of asylum seekers is the extraction of information from mobile devices or 'data carriers', such as smartphones and laptops, that asylum applicants may carry on them. The confiscation of data carriers is currently standard practice in

the Netherlands, optional in Norway and Germany, while it is not used in Belgium and Sweden (EMN 2017b: 32). In the Netherlands and Norway, the aliens police (the AVIM and PU, respectively) confiscate and extract the data carriers, as they have a role in identity establishment; in Germany, this is done by the BAMF (EMN NCP the Netherlands 2017: 45; Klunderud 2017: 13). Where, in the Netherlands and Norway, the aliens police—on the basis of their police mandate—are tasked with establishing or verifying an asylum seeker's identity, this is different in Belgium, Germany and Sweden. Because police authorities are hardly involved in the identification and registration of asylum seekers in these countries, the legal possibilities of extracting information from data carriers are much more limited. Arguably, the actors responsible for identification and registration in Belgium, Germany and Sweden may in addition lack the (police) 'culture' to look for information by means of methods such as extracting data from telephones. This possibly explains why Belgium and Sweden at the moment of our study did not use data-carrier extraction at all and, in Germany, the method can only be used under strict conditions, as will be explained below.

The confiscation and extraction of data carriers are used on the largest scale and in the most far-reaching way in the Netherlands. Since the influx increased, the AVIM subject *all* data carriers to a general check (a staff member takes a 'quick look' by scrolling through the content on the data carrier). Depending on signals resulting from the quick look or other methods used during the identification process, the data carrier may be selected for further investigation, consisting of reading out and extracting all the data on the carrier. According to an inspection report of the Dutch Inspectorate of Justice and Security (2016), Universal Forensic Extraction Devices, or UFEDs, are used for this; they have software that transports data to the authorities' own computers and enables them to analyse this (p. 22). At the time of the publication of the report (November 2016), the number of fully extracted smartphones was about 7 per day on an average of 30 asylum seekers, which was the maximum capacity at the time (*ibid.*: 33). There may also be reasons to submit the data carrier for forensic digital examination by investigative authorities outside the identification and registration process (EMN NCP the Netherlands 2017: 45). Hence, currently, not all confiscated data carriers are also extracted. However, a redesign for the identification and registration process does provide for 100 per cent extraction of data from data carriers (R1). The introduction of the extraction of a limited number of data carriers was possible within the existing legislative context; the terms 'documents and records' laid down in the Dutch Aliens Act 2000 (Article 55(2)) have been interpreted in a broad fashion by judges in relation to the establishment of identity and data carriers are seen to fall within the scope of these terms (EMN NCP the Netherlands 2017: 17). Currently, it is legally not possible to extract data from confiscated data carriers in *all* cases, but only in cases where it is expected that this will produce information that is relevant for assessing the application for a residence permit (personal communication with an officer of the Dutch Aliens Police, 11 December 2019).

In Norway, legislation permits the PU to (temporarily or permanently) confiscate data carriers and access their content in the context of establishing or verifying the identity. Similarly to the Netherlands, these searches are laid down indirectly in the legislation (Klunderud 2017: 13). Checking the content on smartphones already started before 2015, but was initially done on an ad hoc basis (R9, R12). Over time, a more structural approach has been adopted. If the content on the data carriers is to be accessed, the data carrier will be extracted by a specialized digital forensics unit at the PU. The decision to extract information from data carriers is made ad hoc, based on informal criteria. For example, a single Syrian male between the ages of 20 and 40 is very likely to have his phone extracted, even if his documentation does not seem to be problematic. For other nationalities, if applicants have no or clearly forged identity documents, something seems to be wrong with the identity documents or if the applicant's statements lead to doubts about the identity, this may lead to the decision to read out data carriers (R12).

The German BAMF has only recently started extracting data carriers, after amendments to legislation were introduced in 2015 to make this possible (Tangermann 2017: 35). The BAMF can only extract data for the purpose of establishing the identity, but not for other purposes, such as reconstructing the travel route, let alone assessing aspects of national security or 1F exclusion. The software that is used for data extraction does provide information about locations, but does not link this, for example, to time stamps (R39, R40). Furthermore, the method can only be used if no less intrusive method is available (R38). A legal expert from the BAMF needs to assess the proportionality of the storage (or 'validation') of the data because, once the data has been validated, it is analysed by software and the applicant's privacy may be affected. After approval of the use of the method by the legal expert, a report of the analysis is generated and added to the applicant's file (R39). The measure is not allowed when there are indications that analysing data carriers would provide only insights 'into the core area of private life'. If such insights are acquired, they may not be utilized and any records thereof have to be deleted immediately. A written record has to be made of the fact of their acquisition and deletion. Personal data acquired through this method that is no longer necessary for the purpose of establishing the identity or nationality has to be deleted immediately (Tangermann 2017: 22–24).

Based on EU and national data-protection legislation, the applicant's consent is required before data carriers can be extracted. However, such consent is 'relative', meaning that asylum seekers who wish to lodge a successful application in actual practice do not have much 'bargaining power'. Although a refusal to cooperate can in and of itself not be a ground for denying asylum, it will be an element that will be taken into account in the evaluation of the asylum application (R11, R17, R20). In the Netherlands, for example, the IND can reject an asylum application as manifestly unfounded in the event that the third-country national does not cooperate in or even thwarts the establishment of his or her identity (EMN NCP the Netherlands 2017: 52). In Germany, applicants have a general obligation to cooperate in determining their identity. This duty to cooperate was also extended to data carriers: on request, asylum applicants have to present and

hand over all data carriers in their possession that may help to establish their identity and nationality. If the applicant fails to meet this obligation while there are indications that he or she is in possession of data carriers, the authorities can search the applicant and his belongings. The applicant should also hand over passwords or other information necessary to access the devices. In case of refusal, data can also be obtained from telecommunication providers (Tangermann 2017: 21–24).

What Are the Results?

Determining the value of the use of these methods for decision-making may depend on the purpose for which they are used, the (legal) conditions under which they can be used and which actor employs them. This section describes to what extent and in what ways the methods described above have resulted in (improved) identity establishment and identifying national-security or 1F-exclusion indications. As none of the respondents was aware of the existence of any national or comparative evaluations that assess the effectiveness of social-media analysis or data-carrier extraction for these purposes, we will in this regard largely rely on the (subjective) observations made by our respondents.

Identity Establishment

Several authors note that the use of digital surveillance may lead to a change in behaviour among migrants (e.g. Broeders and Engbersen 2007; Jumbert *et al.* 2018). Dekker *et al.* (2018: 7) found evidence that migrants who are aware of surveillance by authorities would stop using social media and smartphones en route (for instance, by turning off the devices or the Wi-Fi signal) because of the surveillance itself or because their smugglers would prohibit the use. Moreover, they expect that it is likely that migrants employ counterstrategies to divert surveillance, by erasing or getting rid of their smartphones before entering the asylum procedure (*ibid.*: 10). Gillespie *et al.* (2016) found migrants were using avatars and pseudonyms to hide their identities on social media and online. Such behaviour is not necessarily intended to trick authorities in destination countries, but may nonetheless problematize screening activities. A *New York Times* article reported that migrants have been commonly asked to provide Facebook passwords at checkpoints in Syria by both government and IS forces, in order to determine their allegiance in the conflict (Brunwasser 2015). Jumbert *et al.* (2018) note that users may have adapted or self-censured the content on their social-media accounts and mobile devices because of this.

Our respondents had different views on whether and how screening of social media and the content of data carriers complements their work in trying to establish an asylum seeker's identity. First, it is noteworthy to mention that different respondents stressed that these methods are not only useful to identify *problems* with regard to a claimed identity, but that it can also make a claim stronger if it is consistent with other information (EMN NCP Belgium 2017: 40; R28, R29). That

said, some respondents believed that, because of the above-presented 'counter-strategies', the value of social-media analysis and data-carrier screening in establishing identity should not be exaggerated, pointing out that they saw a trend where applicants were increasingly showing up without a smartphone or any other personal belongings on them (R7, R14, R15, R16, R38). Some of these same respondents, however, also noted that, as there are few leads in the early phase of the asylum procedure, *any* available lead is valuable and that in particular the method of data-carrier extraction could produce such leads (R14, R15, R16). Other respondents, in particular representatives of the Dutch and Belgium authorities, were more positive about the results and future perspectives of these new screening tools. Representatives of the Dutch IND considered social-media research and data-carrier extraction as very useful, despite possible changes in the use of social media and smartphones by asylum applicants. For a period, there was a suspicion that more applicants were aware that social media was systematically screened and that less information surfaced but, according to respondents, the analysis still produced a lot of useful information. The respondents did report that there had been cases in which they had indications that applicants had set up a fake account as a matter of window dressing or cases in which applicants had several accounts. However, in the experience of Dutch respondents, applicants have to really prepare well to properly conceal that they have set up fake accounts, as data carriers can also be extracted (R31, R32). According to the Belgian EMN NCP, information from social media has proven valuable in particular in cases in which there are doubts regarding the credibility of the asylum motives, country or region of origin or potential exclusion cases.

What furthermore became apparent from the interviews is that the value of information taken from social media regularly is a source of discussion among the immigration authorities. One Norwegian caseworker, for example, referred to discussions with younger colleagues who concluded that an applicant must have been Syrian because they found that he had a Syrian flag as his profile picture and had many Syrian friends (R7). Another Norwegian respondent referred to cases that had been turned down because asylum seekers had claimed to be underage, while it had been found out that their Facebook account mentioned they were 21. The respondent questioned the value of the evidence taken from social media in those cases, as it is not uncommon for young social-media users to present themselves online with a different age, because it may otherwise not be possible to create an account in the first place (R12). German respondents noted that a lot of the information on social media is only available in Arabic and that special interpretation or analysis software is needed to actually make sense of it. More generally, one respondent warned that social-media analysis is of limited use when there is lack of knowledge among caseworkers about how to find information on social media (R7). A particular challenge in Germany has been the size of the influx; doing a proper social-media check on all applicants was simply not feasible. German respondents also referred to problems with regard to privacy protection and legal limitations in collecting and storing personal data (R38, R39).

Finally, we have to stress that, when it comes to information obtained by means of data-carrier extraction, the sharing of such information may lead to complexities. This is in particular apparent in the Netherlands and Norway, where the aliens police are involved in the identification and registration of asylum seekers, but not in the decision-making in asylum procedures. Whether or not—and in what way—the information obtained from data carriers is available and useful for decision-making depends on the ways in which information exchange between the different authorities is organized. Norwegian respondents indicated that this issue has been the subject of intense debate between the PU and UDI. The PU has taken the position that extracted information cannot always be shared with the immigration service, for which reason it draws up selective reports—a very time-consuming activity (R9, R11). UDI representatives indicated that there was a feeling that the amount and quality of information shared by the PU was too selective (R5, E6). In the Netherlands, respondents generally indicated not having experienced many problems in relation to information exchange between the AVIM and the IND.

National Security and 1F Exclusion

Information from open sources and social media is becoming increasingly important in international crimes investigations (Koenig 2017; Human Rights Center UC Berkeley School of Law 2018; Mehandru and Koenig 2019). Due to the increasing availability of smartphones, citizens have easy access to tools to record, document and share evidence via the Internet. These 'citizen witnesses' can offer first-hand accounts, because they are often among the first to be on the scene where crimes occur; if recorded properly, the photos or footage of the crime or crime scene they record may be useful as evidence (Gregory 2015). Asylum applicants may also have photos or footage on their mobile devices or social media incriminating themselves. In fact, visual material found on social-media accounts or mobile devices of immigrants—be it witnesses or perpetrators—has played a decisive role in several terrorism and war-crimes prosecutions with respect to Syria and Iraq that emerged in recent years (especially war crimes of outrage upon personal dignity; see Eurojust 2018), notably in Finland, Germany, Sweden (Eurojust 2018), the Netherlands (District Court of The Hague, judgments of 23 July 2019, ECLI: NL: RBDHA: 2019:7430; and ECLI: NL: RBDHA: 2019:7431; NOS 2019), as well as in a recent case in the situation of Libya before the International Criminal Court (Pre-Trial Chamber I 2017). The fact that such evidence has resulted in criminal convictions illustrates that photos and videos found on social media and mobile devices can be a valuable source for immigration services with respect to identifying national-security threats or 1F-exclusion cases—especially considering that the standard of proof is lower than the criminal-law standard of proof in both 1F-exclusion cases (Fitzpatrick 2000) and national-security cases (in most of the European countries, a danger to the national security is assumed on the basis of an individual report drafted by the national or a foreign intelligence service; assuming such a danger is not dependent on a criminal

conviction). However, from the interviews, it becomes clear that it is not self-evident that these sources of information are in this respect always useful or easily usable.

Various respondents noted that, in general, data carriers and social media are valuable sources of information for assessing national-security or exclusion aspects. A representative of the SMA, for example, indicated that information from these sources is useful in addition to the contextual country-of-origin information (COI) provided by the COI desk, because it is more concrete about individuals (R28; see also Klunderud 2017: 13). Dutch respondents also indicated that information from social media and data carriers is seen as a welcome addition when information from other sources (i.e. statements from applicants) is limited. While they noted that statements by asylum applicants were still the main source for substantiating 1F decisions in the Netherlands, the importance of information from social media was growing. Whether this was also true in the context of national-security assessments, in the Netherlands or in the other countries, cannot be said on the basis of the interviews. The only indication we have of the value of these methods for national-security assessments relates to the 'screening' that is conducted by the IND, of which the social-media research and analysis of data-carrier content are an important part. In a small assessment conducted by the IND on the period from October 2016 to April 2017, it turned out that more than 60 per cent of all signals that were reported to the intelligence services by the IND came from the screening (R34). The remainder of this section therefore focuses on 1F exclusion.

Similarly to establishing an asylum seeker's identity, respondents also indicated that information from social media and data carriers on possible involvement in atrocities or terrorist organizations is often very difficult to interpret and may lead to discussions. As a respondent of the Norwegian Police Security Service (PST) noted: if you see a brutal photo on an applicant's cell phone, is that because he is documenting what is happening during the war or is it his hand holding the knife? (R8). The head of the PST, Erik Haugland, noted the following in an interview with a Norwegian newspaper:

> There may be several reasons for having such images. You can be a witness and want to show others what you have seen, or you may have symbols linked to organizations that control areas you pass through for tactical reasons. What looks alarming can have other explanations than support for terrorist organizations.

He added: 'One problem for us is that we hardly ever have any history of these people, even from countries we work closely with' (Johnsen 2015). Whether the information can be used as evidence for substantiating decisions on asylum applications, particularly in national-security or 1F-exclusion decisions, is therefore not self-evident. A representative of the Norwegian immigration service even noted that the value of information from these sources as evidence is limited. A picture of an applicant with an IS flag in his hand on a public profile, for instance, would never be enough in itself to have a decisive impact on the outcome of a case. At the

same time, the information may still be relevant to actors such as the intelligence and security services (R33). A representative of the Dutch IND gave the example of a Syrian applicant who, during the interview, had claimed to have lived in Damascus his whole life, while pictures had been found of him in the city of Aleppo, dressed in a military outfit and with a Kalashnikov in his hands. Although this information is in itself not enough for exclusion, it does lead to a suspicion that the applicant has 'something to hide' (the limits of what the immigration services can do with information from social media to substantiate 1F decisions are also painfully illustrated in a documentary that was broadcast on Dutch television in 2017; see KRO-NCRV 2017).

The following two 1F-exclusion cases from the Netherlands illustrate how the IND, sometimes successfully and sometimes not, has tried to substantiate 1F-exclusion decisions based on information obtained on social media and other online open sources.

Hell canons

In this case the IND concluded that a Syrian applicant had been involved as a commander in military actions in which 'hell cannons' (heavy improvised weapons) were used against civilians, which amounts to a war crime. The 1F decision—against which the applicant unsuccessfully appealed in court—was based on five different sources of evidence: i) an interview the applicant had given to Associated Press journalists in Greece in which he claimed he had been commander of a rebel faction, ii) his own statements to the immigration services where he inter alia stated he had been a (military) commander and had been involved in founding the Fastaqem Kama Umirt organisation (FKU), iii) images found on the internet: photos depicting the applicant in a military outfit and with a weapon, iv) reports about the military activity of the FKU including the use of hell cannons, and v) a video found on YouTube in which the applicant reads out a statement by the Fastaqem Kama Umirt organisation, after which a hell cannon is loaded and fired and other missiles are fired (District Court of The Hague, judgment of 6 October 2016, ECLI: NL: RBDHA : 2016:12007; judgment of 28 July 2017, ECLI: NL: RBDHA : 2017:9798). In the context of this contribution, it is in particular relevant to stress that the court noted that 'these images strengthen the supposition' that the applicant was involved in the military actions and thus facilitated war crimes. Furthermore, it noted that the fact that his exact involvement in the crimes has not been established in accordance with a criminal law standard is not relevant, as that is not needed for a 1F exclusion (District Court The Hague, judgment of 6 October 2016, pp. 6, 10, 13, translation by authors).

Facebook likes

In a second case, a 1F-exclusion decision was substantiated inter alia by the fact that the applicant's Facebook page showed he was a member of the Syrian Social Nationalist Party (SSNP)—a satellite party of the ruling Ba'ath party—and had placed a 'like' at a photo of members of the air force intelligence service in Aleppo. Furthermore, the IND had found several messages on Facebook, Twitter and other social media in which the Syrian applicant was accused of participating in the

> suppression of demonstrations in Aleppo and supporting the Shabiha militia. Finally, the applicant's name was mentioned on a list of people financing the Shabiha that was available on the website of the Syrian Revolution General Commission (District Court of The Hague, judgment of 8 August 2017, ECLI: NL: RBDHA : 2017:12846, at 9). In this case the District Court ruled that the assumption that the SSNP was to be held accountable for crimes committed by the regime was not substantiated sufficiently. Furthermore, from the information found on the internet and social media, the court reasoned that it does not become clear that the applicant was personally involved in the suppression of demonstrations. That he was accused on social media of involvement in the Shabiha and killing demonstrators is not enough to establish his personal involvement, as these sources cannot be considered to be objective and 'everyone can post messages there'. That the applicant 'liked' a photo of members of the air force intelligence service also cannot lead to the conclusion that he was involved in crimes committed by the regime. Finally, the court considered that if it were likely that the applicant indeed supported the Shabiha financially, this in itself is not enough to conclude he facilitated 1F crimes. The court noted that the applicant's uncooperative attitude is insufficient to come to such a conclusion (*ibid*.: 11).

These examples show that information from social media may raise a suspicion that someone has been involved in 1F crimes, but the information still needs to be sufficiently specific about the individual's role to be suitable as supporting evidence. However, a Dutch respondent noted that the 'classic' substantiation of exclusion decisions detailing the crime, place and time is hardly achievable anymore, given the decreasing value of applicants' statements (R34), as also noted above. This led the IND to adopt a different approach in substantiating 1F-exclusion decisions. While the Dutch immigration service would typically focus on substantiating that the applicant was a member of a certain organization and that this organization has been guilty of 1F crimes, in the new approach, the reasoning is 'turned around'. For instance, it is now argued that the sum of the fact that (i) someone was at a certain location where he had no business, (ii) in a uniform, (iii) with a weapon in his hand, combined with the fact that (iv) he has made implausible or demonstrably untruthful statements about this event, leads to the supposition that there is no other explanation than to assume the applicant has (actively) participated in an armed conflict in which war crimes have been committed, which could be enough to constitute 'serious reasons for considering' that the applicant committed (or facilitated) 1F crimes. At the time of data collection, the IND was trying to find out to what extent this way of motivating an exclusion decision is accepted in court. The respondent acknowledged that this leads to the question of whether the threshold for exclusion is de facto lowered. The IND, however, reasons that the approach has changed, but the standard of proof remains the same. Increasingly, use is made of legal advisers in drafting exclusion decisions, in order to translate information from images into evidence for a judge to review (R34).

Social-Media Analysis and Data-Carrier Extraction: The Way Forward?

As discussed above, the use of social-media analysis and data-carrier extraction to vet asylum seekers has increased over recent years, in the context of both identity establishment and screening on national-security and 1F-exclusion aspects. Based on the interviews that we conducted, the first experiences with both of these new methods seem to be mixed. It is striking to note that there seem to be 'believers' and 'non-believers' in these methods. As became clear in the previous section, representatives from countries that more actively use these methods or have more legal powers to use them, such as the Netherlands and Norway with regard to reading out data carriers, are generally positive about the possibilities and results, while representatives from countries that use these methods to a lesser extent or do not have the legal possibilities to do so, such as Belgium and Sweden with regard to data-carrier extraction, are more sceptical and refer to various—presumed—disadvantages. Assessments of the value of information obtained through these new methods are so far based mainly on anecdotal evidence, rather than systematic evaluations. The use of the methods may lead to adaptations in behaviour of asylum seekers, and so increasing reliance on them may undermine the effectiveness and diminish the results of the methods. In the context of screening on 1F-exclusion aspects, the evidentiary value is also not self-evident, as was illustrated above. In absence of other means to collect sufficient evidence to assess asylum applicants' involvement in crimes, it is understandable that immigration authorities are increasingly exploring whether and to what extent they can use 'digital evidence'. As illustrated above, criminal prosecutors currently use similar approaches in trying to hold returning foreign fighters or asylum seekers and other migrants criminally accountable for involvement in atrocities or terrorism in the Middle East. It is also understandable that immigration authorities are testing new ways to substantiate 1F-exclusion decisions. In this regard, however, considering the serious consequences for individuals who are excluded on the basis of Article 1F (Reijven and Van Wijk 2014), care should be taken in reaching conclusions based on information that is often inconclusive.

To independently assess whether or not the presumed costs of social-media analysis and data-carrier extraction outweigh the possible benefits is currently virtually impossible. The costs—in terms of human resources dedicated to perform social-media screening and setting up systems to enable data-carrier extraction and analyse all the obtained data—are certainly substantial. The benefits—in terms of improved identity establishment and improved screening of national-security and 1F-exclusion cases—are of yet 'sketchy' at best and based on anecdotal evidence. One indication of the balance between costs and benefits can be deduced, however, from answers provided by the German BAMF to questions from the opposition party, Die Linke (see Thüer *et al.* 2018). According to the provided information, in 9 months from September 2017, BAMF extracted data from mobile devices of almost 15000 persons unable to produce any identity papers. In approximately one-third of the approximately 5000 cases for which the information was actually accessed, the data supported the information

provided by the applicants; in almost two-thirds the BAMF concluded the information was not relevant in terms of establishing identity and origin; and in only around 100 cases did the data contradict what the applicant had stated initially. Thüer *et al.* (2018) argue that, given that approximately 230000 asylum applications were decided in this period, this result is disproportional to the investments made in the technology and the infringement on the privacy of applicants. Furthermore, the figures also suggest that the measure is not used only as a 'last resort', as required by law. Based on the interviews, the authors have the impression that sound evaluations with proper cost–benefit analyses of these new methods are not—or at least not publicly—available. This impairs a fact-based and normative debate on whether or not, and to what extent, the implementation of such methods is recommendable. Hence, there is a clear need for such evaluations.

Apart from questions regarding effectiveness and cost-efficiency, the increasing reliance on these methods, in combination with the further advancement of technology, raises a number of practical, legal, normative and ethical questions that are currently hardly (publicly) discussed. As for the increasing reliance on social-media research in the immigration context, there seem to be no fundamental objections against per se, but practical improvements are possible and it does raise some legal and ethical concerns. Respondents in our study, for example, indicated that guidelines on 'who does what' are not always available. Moreover, as one respondent mentioned, the boundary of how far and by which means a non-investigative administrative authority such as the immigration authority may employ such searches in examining an immigration or asylum case is increasingly blurred (R11). One observation that can be made from our study is that immigration services—in line with the developments described in 'crimmigration' literature (Stumpf 2006; Van der Woude *et al.* 2017)—are gradually taking steps to move closer towards conducting criminal investigations. The special computers that the Dutch IND uses to perform social-media analysis, which have been developed by the National Police, are an illustration of this development. The gradual move in the direction of criminal investigation, resulting from pressure from politics and the society, means that the expectations from immigration authorities are higher, although it is yet unclear whether they—even with these increased investigative tools—can actually 'live up' to these expectations. The use of anonymous or 'fake' Facebook accounts to perform social-media searches could perhaps be seen as problematic, but one might argue that applicants cannot credibly object to the use of information that they have consciously disclosed to the public. It becomes more questionable when immigration authorities engage in the vetting of non-public parts of social media. As Meaker (2018) describes, the Danish immigration authorities ask asylum applicants in some cases to provide their Facebook passwords so that they can access what cannot be easily found; upon refusal, the applicant will be told that he is obliged to cooperate under Danish law. The US immigration authorities have already implemented a policy whereby (even) *visa* applicants are required to submit information about social-media accounts they have used in the past (Garcia 2019).

However, it is especially the vetting of mobile 'data carriers' such as smartphones that raises serious legal, normative and ethical concerns. Over time, the data-storage capacities on these devices have increased and the number of applications for which these can be used is growing. As a result, these mobile devices contain more and more personal information. Confiscating and extracting data from such devices today thus implies a strong infringement on the right to a private life as protected by Article 8 of the European Convention on Human Rights (Royer and Oerlemans 2017: 280). In particular, in countries where there is no sound legal basis or when it can be proven that the applied methods are not effective in reaching its objectives (lack of proportionality), it may even be in violation of European or national legislation.

It is interesting to note the differences between the focus countries when it comes to the extent to which privacy considerations played a role in the introduction of data-carrier research. As noted above, in the Netherlands, the introduction of the method was deemed possible within the existing legislative framework. Consequently, the introduction was not discussed in parliament; it went by largely unnoticed and did not create much public or political upheaval. In Belgium and Germany, on the other hand, legislative changes were required and their introduction led to considerable debate. In Germany, different organizations voiced data-protection concerns in reaction to the announcement of the introduction of data-carrier extraction. For instance, opposition party Die Linke ('The Left') described the method as 'an infringement on citizen's rights, seeing that mobile phones could be analysed without a court order even if there was no suspicion of a crime'. The opposition party Bündnis 90/Die Grünen ('Alliance 90/The Greens') opposed that the scope of the method was ill-defined. Civil-society organizations were critical about the way in which the use of these methods would affect the (confidential) relationship during interviews with the BAMF (Biselli 2017; Tangermann 2017: 49). Respondents in our study also indicated that data protection in general is a sensitive issue in Germany (R38, R39, R40). These factors could explain the relatively strict conditions under which, and the limited purpose for which, the method can be used. In Belgium, the introduction of the competence to extract information from data carriers by the CGRS was preceded by extensive debate in parliament and society on the issue of whether accessing information on data carriers was only possible after approval of the applicant or whether such cooperation could also be enforced. The Belgian Privacy Commission in this regard issued negative advice on the initial proposal, criticizing it for lacking provisions on how applicants would be asked to give access to data carriers in their possession, how the collected data would be stored and how it would be analysed. The UNCHR was also critical on the issue of the applicant's consent (R20; EMN NCP Belgium 2017: 60). As a result of this debate, the law, in its final form, requires that access to data carriers can only be obtained on the basis of the applicant's consent (R17, R20). However, as noted above, applicants may not have much leeway to refuse their cooperation in this sense. It has been argued that, when permission is asked by an entity that is in a position of power over the

individual or the individual is not in a position to disagree, this can in fact not be qualified as 'consent' (Privacy International 2019).

Apart from privacy issues, concerns could be raised regarding data protection and the potential use of information initially gathered for the purpose of identity establishment at a later stage for different purposes—the risk of a so-called 'function creep' (Brouwer 2011: 274). One example of function creep, already referred to by Brouwer (2011: 282), is the access to the Eurodac fingerprint database that law-enforcement authorities have had since 2015 for comparison with fingerprints in law-enforcement databases. This database was once established solely for the purpose of determining the EU Member State responsible for asylum applications, but can now under certain circumstances be used for law-enforcement purposes (Regulation (EU) No. 603/2013 of the European Parliament and of the Council of 26 June 2013). The amount of (personal) data on modern-day mobile devices can be enormous and they may therefore be a valuable source for authorities, but it is questionable whether the use of data for anything other than the limited purpose for which it was gathered is actually legitimate.

Another issue relates to the question of how to analyse all the gathered data. While the immigration authorities currently still only have the capacity to use data-carrier extraction selectively, the Dutch aliens police aims at 100 per cent data-carrier extraction in the near future (Thüer *et al.* (2018) report that similar legal possibilities have been created in Austria). All of this data will be stored in a central database. Tools are currently being developed to systematically search this data using specially developed queries, based on indicators or profiles of persons who may pose a risk, albeit not by the aliens police, but by the counterterrorism police (R1). This raises the potential for 'social sorting', i.e. the identification of certain groups posing a risk based on certain criteria or categories, which could have self-reinforcing effects and thus lead to discrimination (Das and Schuilenburg 2018; Jumbert *et al.* 2018).

Some of the developments described above, such as the increased extraction of information from data carriers and the development of smart tools to analyse the obtained 'big data' by governmental authorities but also by commercial companies (companies such as T3K, MSAB and Cellebrite; see Meaker 2018; Privacy International 2019), perfectly fit the development of what some authors have referred to as the 'EU Security-Industrial Complex' (TNI and Statewatch 2017). With regard to immigration management, the EU and European countries increasingly modify legislation, develop new strategies and invest large amounts of money in developing and building technologies to ensure the security of EU citizens. This study on social-media and mobile-device vetting in asylum procedures provides an illustration of these developments. At the same time, it is questionable to what extent the steps taken are proportional to the results of these efforts and to what extent fundamental human rights, including privacy, are sufficiently safeguarded. It is therefore imperative to have more public, evidence-based discussions about these issues on a national as well as a European level.

Acknowledgements

The most substantial part of the data collection was conducted as part of a research project funded by the Norwegian Directorate of Immigration UDI. The authors thank Evelien Brouwer and the two anonymous reviewers for their valuable comments on an earlier draft.

ALENCAR, A., **KONDOVA, K.** and **RIBBENS, W.** (2018) 'The Smartphone as a Lifeline: An Exploration of Refugees Use of Mobile Communication Technologies during Their Flight'. *Media, Culture and Society*, 41(6): 828–844.

BISELLI, A. (2017) 'Digitalisierte Migrationskontrolle: Wenn Technik Über Asyl Entscheidet', *Burgerrechte & Polizei/CILIP* 114 (11/2017), https://www.cilip.de/2017/11/23/digitalisierte-migrationskontrolle-wenn-technik-ueber-asyl-entscheidet (accessed July 2019).

BOLHUIS, M. P. and **VAN WIJK, J.** (2018) *Case Management, Identity Controls and Screening on National Security and 1F Exclusion: A Comparative Study on Syrian Asylum Seekers in Five European Countries. Final Report of a Study Commissioned by the Norwegian Directorate of Immigration, UDI*. Amsterdam: VU University.

BOLHUIS, M. P. and **VAN WIJK, J.** (2019) 'Practices in Establishing the Identity and Screening on National Security and Exclusion Aspects in Syrian Asylum Cases in Five European Countries'. *Migration Policy Practice* IX(2): 13–17.

BROEDERS, D. and **ENGBERSEN, G.** (2007) 'The Fight against Illegal Migration Identification Policies and Immigrants' Counterstrategies'. *American Behavioral Scientist* 50(12): 1592–1609.

BROUWER, E. (2011) 'Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation'. In Besselink, L., Pennings, F. and Prechal, S. (eds) *The Eclipse of the Legality Principle in the European Union*. Alphen aan den Rijn: Kluwer Law International, pp. 273–294.

BRUNWASSER, M. (2015) 'A 21st-Century Migrant's Essentials: Food, Shelter, Smartphone', *New York Times*, 25 August, https://www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=1 (accessed July 2019).

COMMISSIONER GENERAL FOR REFUGEES AND STATELESS PERSONS (CGRS) (2017) *Presentation by a Representative of the CGRS* [video], https://www.udi.no/en/statistics-and-analysis/european-migration-network---norway/conferences-and-events/conferences/the-use-of-methods-and-technology-in-identity-verification-2017/ (accessed July 2019).

DAS, A. and **SCHUILENBURG, M.** (2018) 'Predictive Policing: waarom Bestrijding Van Criminaliteit op Basis Van Algoritmen Vraagt om Aanpassing Van Het Strafprocesrecht'. *Strafblad*, October: 19–26.

DAWAR, A. (2015) 'Alarm as Syria Sells 10,000 Passports with Few Questions Asked', *Express*, 11 September, https://www.express.co.uk/news/world/604394/Alarm-Syria-sells-10000-passports-few-questions-asked (accessed July 2019).

DEKKER, R. and **ENGBERSEN, G.** (2014) 'How Social Media Transform Migrant Networks and Facilitate Migration'. *Global Networks* 14(4): 401–418.

DEKKER, R., **ENGBERSEN, G.** and **FABER, M.** (2016) 'The Use of Online Media in Migration Networks'. *Population, Space and Place* 22(6): 539–551.

DEKKER, R., **ENGBERSEN, G.**, **KLAVER, J.** and **VONK, H.** (2018) 'Smart Refugees: How Syrian Asylum Migrants Use Social Media Information in Migration Decision-Making'. *Social Media + Society* 4(1): 205630511876443.

EMMER, M., **RICHTER, C.** and **KUNST, M.** (2016) *Flucht 2.0. Mediennutzung Durch Flüchtlinge Vor, Während und Nach Der Flucht*. Berlin: Freie Universität Berlin.

EMN (EUROPEAN MIGRATION NETWORK) (2016a) *Ad-Hoc Query on the Criteria for Application of Exclusion Clause—Danger to the Community and Danger to the State Security—While Reviewing the Applications for International Protection Requested by Slovakian EMN NCP on 6th September 2016*, http://www.emnitalyncp.it/wp-content/uploads/2018/02/070_b_sk_the_criteria_for_application_of_exclusion_clause.pdf (accessed July 2019).

EMN (2016b) 'The Use of Social Media in the Fight Against Migrant Smuggling', *EMN Inform*, September, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/reports/docs/emn-informs/emn-informs-00_emn_inform_on_social_media_in_migrant_smuggling.pdf (accessed July 2019).

EMN (2017a) *EMN Ad-Hoc Query on Mobile Device Information, Requested by Austrian EMN NCP on 9th May 2017*, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/2017.1180_at_mobile_device_information.pdf (accessed July 2019).

EMN (2017b) *Synthesis Report for the EMN Focussed Study 2017, 'Challenges and Practices for Establishing the Identity of Third-Country Nationals in Migration Procedures'*, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_synthesis_report_identity_study_final_en.pdf (accessed July 2019).

EMN NATIONAL CONTACT POINT [NCP] BELGIUM (2017) *Challenges and Practices for Establishing Identity in the Migration Process in Belgium, Study of the Belgian Contact Point of the European Migration Network (EMN)*, https://emnbelgium.be/publication/challenges-and-practices-establishing-identity-migration-process-emn (accessed July 2019).

EMN NCP THE NETHERLANDS (2017) *EMN Focussed Study 2017 Challenges and Practices for Establishing Applicants' Identity in the Migration Process*, on file with the authors.

EUROJUST (2018) *Prosecuting War Crimes of Outrage Upon Personal Dignity Based on Evidence from Open Sources—Legal Framework and Recent Developments in the Member States of the European Union*. The Hague: Eurojust, http://www.eurojust.europa.eu/doclibrary/genocide-network/KnowledgeSharing/Prosecuting%20war%20crimes%20of%20outrage%20upon%20personal%20dignity%20based%20on%20evidence%20from%20open%20sources%20(February%202018)/2018-02_Prosecuting-war-crimes-based-on-evidence-from-open-sources_EN.pdf (accessed July 2019).

EUROPOL/EUROPEAN MIGRANT SMUGGLING CENTRE (EMSC) (2017) *First Year Activity Report*. The Hague: Europol/EMSC.

EZADI, E. (2015) 'There's a Booming Black Market for Fake Syrian Passports', *Washington Post*, 21 November 2015, https://www.washingtonpost.com/news/worldviews/wp/2015/11/21/theres-a-booming-black-market-for-fake-syrian-passports/? utm_term=.d37171b9166a (accessed July 2019).

FITZPATRICK, J. (2000) 'The Post-Exclusion Phase: Extradition, Prosecution and Expulsion'. *International Journal of Refugee Law Special Law* 12(Suppl 1): 272–294.

GARCIA, S. E. (2019) 'U.S. Requiring Social Media Information from Visa Applicants', *New York Times*, 2 June 2019, https://www.nytimes.com/2019/06/02/us/us-visa-application-social-media.html (accessed July 2019).

GILLESPIE, M., **AMPOFO, L.**, **CHEESMAN, M.**, **FAITH, B.**, **ILIADOU, E.**, **ISSA, A.** *et al*. (2016) *Mapping Refugee Media Journeys. Smartphones and Social Media Networks*. Paris: The Open University/France Médias Monde.

GREGORY, S. (2015) 'Ubiquitous Witnesses: Who Creates the Evidence and the Live(d) Experience of Human Rights Violations?'. *Information, Communication & Society* 18(11): 1378–1392.

HACSEK, Z. and **VISNANSKY, B.** (2017) *The Impact of Social Media on the Smuggling of Migrants*, Regional Academy of the United Nations, http://www.ra-un.org/uploads/4/7/5/4/47544571/2_unodc_2_final_paper.pdf (accessed July 2019).

HAMEL, J.-Y. (2009) *Information and Communication Technologies and Migration*, United Nations Development Programme, Human Development Reports, Research Paper 2009/39, https://mpra.ub.uni-muenchen.de/19175/1/MPRA_paper_19175.pdf (accessed July 2019).

HUMAN RIGHTS CENTER UC BERKELEY SCHOOL OF LAW (2018) *The New Forensics: Using Open Source Information to Investigate Grave Crimes*, https://www.law.berkeley.edu/wp-content/uploads/2018/02/Bellagio_report_2018_9.pdf (accessed July 2019).

IMMIGRATIE EN NATURALISATIEDIENST (IND; NETHERLANDS IMMIGRATION SERVICE) (2016) 'Screenen in het Asielproces. IND-interne basisinstructie voor de screener', version 1.0, 8 March, copy on file with the authors.

INSPECTIE JUSTITIE EN VEILIGHEID (INSPECTORATE OF JUSTICE AND SECURITY) (2016) *De identificatie van asielzoekers in Nederland: Vervolgonderzoek naar de Registratie en Identificatie van Asielzoekers door Politie en Koninklijke Marechaussee*. The Hague: Inspectie Justitie en Veiligheid.

JOHNSEN, N. (2015) 'Slik overvåker PST asylstrømmen', 13 December, https://www.vg.no/nyheter/innenriks/i/429Bo/slik-overvaaker-pst-asylstroemmen (accessed July 2019) (translated by authors).

JUMBERT, M. G., **BELLANOVA, R.** and **GELLERT, R.** (2018) 'Smart Phones for Refugees: Tools for Survival, or Surveillance?'. *PRIO Policy Brief* 04/2018.

KLUNDERUD, K. (2017) *EMN Synthesis Report for EMN Focused Study 2017: Challenges and Practices for Establishing the Identity of Third-Country Nationals in Migration Procedures—Report from Norway*, https://www.udi.no/globalassets/global/european-migration-network_i/studies-reports/emn-id--norwegian-response.pdf (accessed July 2019).

KOENIG, A. (2017) 'Harnessing Social Media as Evidence of Grave International Crimes', Human Rights Center UC Berkeley School of Law blog, 23 October, https://medium.com/humanrights center/harnessing-social-media-as-evidence-of-grave-international-crimes-d7f3e86240d (accessed July 2019).

KRO-NCRV (2017) 'Het Kaf en het Koren', 10 April, https://www.2doc.nl/documentaires/series/2doc/2017/april/het-kaf-en-het-koren.html (accessed July 2019).

MARSH, R. (2015) 'U.S. Report Warns of ISIS' Ability to Create Fake Passports', *CNN*, updated 11 December, https://edition.cnn.com/2015/12/11/politics/isis-passports/ (accessed July 2019).

MEAKER, M. (2018) 'Europe Is Using Smartphone Data as a Weapon to Deport Refugees', *Wired*, 2 July, https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations (accessed July 2019).

MEHANDRU, N. and **KOENIG, A.** (2019) 'Open Source Evidence and the International Criminal Court', Harvard Human Rights Journal blog, 15 April, https://harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/ (accessed July 2019).

NOS (2019) 'Syriër aangehouden in Ter Apel voor vernederen dode tegenstanders', 25 October, https://nos.nl/artikel/2307619-syrier-aangehouden-in-ter-apel-voor-vernederen-dode-tegenstanders.html (accessed July 2019).

PRE-TRIAL CHAMBER, I. (2017) 'Arrest Warrant in the Case of the Prosecutor v. Mahmoud Mustafa Busayf al-Werfalli', 15 August, https://www.icc-cpi.int/CourtRecords/CR2017_05031.PDF, §§11–22 (accessed July 2019).

PRIVACY INTERNATIONAL (2019) 'Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers', https://www.privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers (accessed July 2019).

REIJVEN, J. and **VAN WIJK, J.** (2014) 'Caught in Limbo: How Alleged Perpetrators of International Crimes Who Applied for Asylum in the Netherlands Are Affected by a Fundamental System Error in International Law'. *International Journal of Refugee Law* 26(2): 248–271.

ROYER, S. and **OERLEMANS, J. J.** (2017) 'Naar Een Nieuwe Regeling Voor Beslag op Gegevensdragers'. *Computerrecht* 200(5): 277–284.

SCHANS, D. and **OPTEKAMP, C.** (2016) *Raising Awareness, Changing Behavior? Combatting Irregular Migration through Information Campaigns*. The Hague: Research and Documentation Centre, Ministry of Justice and Security (WODC), https://www.wodc.nl/binaries/Cahier%202016-11_2683_Volledige%20tekst_tcm28-239610.pdf (accessed July 2019).

STUMPF, J. P. (2006) 'The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power'. *American University Law Review* 56(2): 367–420.

TANGERMANN, J. (2017) *Documenting and Establishing Identity in the Migration Process: Challenges and Practices in the German Context. Focussed study by the German National Contact Point for the European Migration Network (EMN)*, Working Paper 76, http://www.bamf.de/SharedDocs/Anlagen/EN/Publikationen/EMN/Studien/wp76-emn-identitaetssicherung-feststellung.pdf?__blob=publicationFile (accessed July 2019).

THÜER, L., **FANTA, A.** and **KÖVER, C.** (2018) 'Asylum Procedure: Cell Phone Search Has No Benefits', UNHCR blogs, 16 July, https://www.unhcr.org/blogs/asylum-procedure-cell-phone-search-no-benefits/ (accessed July 2019).

TRANSNATIONAL INSTITUTE (TNI) and STATEWATCH (2017) *Market Forces: The Development of the EU Security-Industrial Complex*, https://www.tni.org/files/publication-downloads/marketforces-report-tni-statewatch.pdf (accessed July 2019).

VAN DER WOUDE, M. A. H., **BARKER, V.** and **VAN DER LEUN, J. P.** (2017) 'Crimmigration in Europe'. *European Journal of Criminology* 14(1): 3–6.

ZIJLSTRA, J. and **VAN LIEMPT, I.** (2017) 'Smart(Phone) Travelling: Understanding the Use and Impact of Mobile Technology on Irregular Migration Journeys'. *International Journal of Migration and Border Studies* 3(2/3): 174–191.