Notes from EMN Norway's National Conference

The use of Technology in Identity Verification

Oslo, Thursday 1 June 2017

The agenda for the Conference is Annex I to these notes, and the speakers are presented in Annex II.

Jan-Paul Brekke, senior researcher at the I*nstitute of Social Research (ISF)*, acted as moderator.

The participants were greeted by ***Mr. Fabian Stang***, State Secretary in the *Ministry of Justice and Public Security*, who welcomed them to the conference and to Oslo. As a former major of the city he offered to advise foreign guests on what to see and visit if they decided to stay after the close of the conference.

Using the *Facebook* as an example **Kris de Groot**, senior researcher at *CEDOCA, the country of origin information (COI) desk at the Commissioner-General's Office for Refugees and Stateless* in Belgium, presented the challenges and possibilities for using searches on social media to verify or establish a person's identity, e.g. someone applying for a visitor's visa or for protection, taking advantage of the fact that almost everything that someone has placed on the medium will be publicly available with the right search tools.
Even when someone has made use of a privacy protection facility on the medium, the information may become public through a 'friend's' profile, if s/he has not invoked that facility. While the postings of members of a 'closed group' may not be public, the membership of the group is public, and that may be significant in an effort to establish the identity of an individual member.
In BE all case workers are given basic training in *Facebook* search. Advanced training is given to specialized units investigating fraud, radicalization, etc. The social media search activities are supported by a *New Media Unit*, a small team of specialized COI researchers.

Maria Gabrielsen Jumbert, research director and senior researcher at the *Peace Research Institute, Oslo (PRIO)*, presented ethical, legal and humanitarian perspectives on the digital migrant, focusing on the authorities' examination of migrants' electronic devices in their efforts to verify or establish their identity.
Smartphones have proved to be an essential tool for migrants and refugees when seeking to reach their destinations, as well as for obtaining and sharing vital information, and support groups have focused on providing infrastructure such as wifi points and recharging stations. Questions have been asked about a person's real need for protection if s/he can afford having and using a smartphone. The information generated by the migrant's use of a smartphone may be used for other purposes, e.g. by the government seeking (to verify) information, and this generates ethic, legal and humanitarian issues.
Potential (governmental) uses are (i) verification of information provided by a migrant; and (ii) investigate whether s/he may represent a security threat. Questions then raised include: Can the information on the digital device be trusted to reflect the 'true' identity of someone

(claiming to be) fleeing persecution? Has there been one unique user or several of a particular device? How does the authorities' use of information from digital devices influence how these are used? Do the authorities risk reliance on incorrect or incorrectly interpreted information? What is the right of appeal for an individual when a decision is based on information gained from search on social media? Is there a disproportionate asymmetric power relationship between the migrant and the authority?

Issues related to cross border digital identity in the EU were presented by ***Philippe van Triel*** from the *Unit Information Systems for Borders and Security, DG Home, European Commission.* The point of departure for his presentation was that the relevant legislation is concerned with specific, identifiable individuals. One challenge is that the identification of a person cannot rely on his/her name or an ID-document. Biometrics are needed, even if there is a small risk (less than 1 percent) that with biometrics s/he may be confused with someone else or not recognized.
For border control (management and surveying) EU has established a database (VIS) with biometric information (face and fingerprints) for all TCN applying to visit a Schengen member country, and another (EURODAC) for asylum seekers in Dublin member countries, but there is no EU system for biometrics with longer term residence permits issued to TCNs.
The Schengen information System (SIS) ties all relevant national information systems to a central one for Schengen member states, alerting national authorities to the possibility that a Schengen visitor's visa may be requested by a TCN that is undesirable in one of the member states, e.g. because of an entry ban. Introduction of fingerprint recognition capabilities in SIS will reduce the danger that a visa may be issued to such individuals, or that someone will be wrongly denied a visa.
There are plans for establishing an entry/exit registration system for all TCNs crossing an external Schengen border. This will assist in identifying 'over stayer' (but not their location) and contribute to the fight against terrorism and other crimes committed by TCN on Schengen territory.
The citizens of many countries are visa-exempt. For those there are plans to introduce a system for (pre-)travel authorization.
There are plans for an EU integrated identity management capacity that will embrace SIS, VIS and EURODAC, and establish an identity depository on the basis of ID information from these systems.

Kathrine Qvenild from the *Norwegian Directorate of Immigration (UDI)* presented plans for developing biometrics and data sharing in Norway. Norway is party to SIS and EURODAC, but so far only providing biometric data to these system: the basis for systematic sharing of such data between agencies and analysing them has not been in place, but is now being developed by UDI, the *Police* and the *Ministry of Foreign Affairs* in a joint project, that is managed by UDI. The biometric information will be captured when applications are made for residence permits (fingerprints from age 6), Schengen visa (fingerprints from age 12 and/or protection (fingerprints from age 15). (The legal basis is §100 in the Immigration Act.) One aim is to ensure that every TCN has only one identity in Norway.
For an applicant there will be advantages: reuse of saved biometrics; less need for several appearances at foreign service missions; better protection of privacy because of stricter rules for storage and access; reuse of the police solution for passports and the new national ID-cards.
Existing biometric registrations will be 'cleaned' to reduce the danger of introducing errors and data with sub-standard quality. There is also a project for e.g. modernizing the

Database of Foreigners (UDB), the registration system DUF and their links to the *National Central Population Register*.
Following these presentations the moderator invited comments and questions from the audience. These included:

- Why only short term visitor's visa in VIS and EES? (The competence of EU.)
- Ethical issues in harvesting data from social networks? (Only data in the public domain are harvested.)
- Possibility for establishing an EU wide register of the citizens of its member states? (Outside the competence of EU.)
- The prevalence of fake profiles on social networks. (Quite frequently encountered.)

Bronwen Manby, researcher at *London School of Economics,* provided insights into practical realities of national identification systems in Africa, providing facts and figures on official identification registrations and documentation in several countries. The number of systems (formally) in place have increased significantly during recent years. However, birth registration rates are generally low, and very different between rural and urban areas. It is almost impossible to obtain documentation of a birth that have happened a little while ago, and a birth registration does not document nationality. For adults there are several different forms of registrations (voter, driving license, ID-card, passport). Theoretically there may be national systems, but in practice it is only some very local systems that are functional, but even they (generally) do not document nationality.
Very different and complicated nationality laws exist, which frequently discriminate against certain groups, defined e.g. by gender, parentage, ethnic group, place of birth (may be a consequence of state successions at independence or later). The civil registration systems are very weak, if they exist, with few possibilities for late birth registrations, harsh conditions for obtaining ID cards (e.g. vetting on the basis of grandparents, or only against high official and unofficial costs. Risk of statelessness is high for migrants and their descendants (pre-independents as well as contemporary), and for cross border populations.
Identification systems in Africa effectively depend on witness testimony. Biometric identification may have many uses, but cannot tell who is a national of country X. To determine a person's nationality in country X is partly a question of law, but perhaps even more so a question of practical realities.

Per Haddal from the *Norwegian Identity Centre* discussed how to ensure a holistic approach to identity verification and determination, given that a large number of ID-documents still are awaiting verification to establish whether they are genuine, provide correct information and can be convincingly linked to the person presenting them. Such tasks are complicated and develop dynamically as technology for falsification and verification changes. Resources and time available limit the possibilities for catching all, or even a large proportion of, efforts to misuse ID-documents. It is, however, possible to simplify expensive and complicated laboratory document examinations with processes that do not seriously jeopardize the quality of the outcome. An early screening by experienced document examiners to identify high risk cases can eliminate a large proportion of 'suspect' documents (up to 90 percent) from detailed examination, even though it may become relevant to return to them later if new information has been forthcoming. Most efforts may then be spent on high risk cases, making the whole process more effective in terms of time and resources. Information sharing between experts and agencies will help opening a tool box otherwise only half open. An important challenge

for linking a person to a correct and credible ID-document is to have an unbroken chain from the first breeder document (e.g. a birth certificate) to the ID-document issued.

Sveinung Hilmy Wetteland from the *National Police Immigration Service's (PU)* forensic unit discussed immigration through the digital eye, i.e. how digital forensics play a role in assessing the merits of the case presented by an asylum seeker. The starting points are the name and alias, friends and family, cloud accounts and user ID, photos taken by PU and in any ID-documents presented or found, digital devices (smartphones, laptops, tablets, SIM-cards). From the digital devices one may obtain the device user name, location data (true or false), media accessed (with meta data), communications (to/from where), applications, user accounts, internet streaming and storage of information (open sources and information behind walls for pay or for other reasons). A condition for gaining access may be to have a good understanding the environment of the device, and its use.